МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет
«Харківський політехнічний інститут»

А.А. Бадан

ПЕРЕКЛАД АНГЛОМОВНИХ ТЕКСТІВ У ГАЛУЗІ ІНФОРМАЦІЙНИХ БАНКІВСЬКИХ ТЕХНОЛОГІЙ

Навчальний посібник
для студентів та аспірантів спеціальності 6.020303 «Переклад»

Затверджено редакційно-видавничою
радою університету,
протокол № 2 від 06.12.2012 р.

Харків
НТУ «ХПІ»
2013

УДК 088.8:03:811.111
ББК 30у:81.2
Б 18

Рецензенти: *Н.М..Лисиця*, д-р. соціол. наук, проф. кафедри економіки і маркетингу Харківського національного економічного університету;
В.М.Сердюк, канд. філол. наук, доц. Харківського національного університету ім. В.Н.Каразіна.

У навчальному посібнику використано оригінальний англомовний матеріал у галузі інформаційних банківських технологій. Висвітлено англомовну термінологію у вказаній галузі і подано зразки англомовних слів та виразів, що необхідні для подальшої роботи під час виконання вправ. Зручний до використання двомовний англо-український словник, що охоплює усі модулі, розташований у кінці книги. Система вправ є циклічною для кожного модуля і призначена для автоматичного засвоєння вміння перекладу слів та виразів, а також для навчання кваліфікованого англо-українського перекладу банківських текстів, що пов'язані з використанням інформаційних технологій.

Для студентів перекладацьких відділів та фахівців з перекладу у галузі економіки та комп'ютерних технологій.

Бадан А. А.
Переклад англомовних текстів у галузі інформаційних банківських технологій : навч. посіб. / А.А. Бадан. – Х. : НТУ "ХПІ", 2013. – с. – Англ. та укр. мовами.

ISBN

The manual is built on the authentic material in English in the field of information banking technologies. It highlights the English terminology in the above field and gives examples of English words and phrases necessary for further mastering while doing the exercises. The Ukrainian-English glossary which is conveniently set at the end of the manual comprises all the modules given.

The system of exercises is of a cyclic character for each module and intended for working up automatic skills of translating words and phrases, as well as for training qualified English-Ukrainian translation of banking texts based on information terminology.

Compiled for translation students and experts in economic and computer-aided technologies translation.

Bibl. 8 titles.

УДК.088.08:03
ББК 30у:81.2

ISBN

Зміст

Вступ

Термінологія у галузі інформаційних банківських технологій виникла одночасно з упровадженням високих технологій у банківську систему і швидко розвивається. Особливості цієї термінології полягають у комбінації економічних та комп'ютерних (суто технічних) понять, що зумовлює появу унікального термінологічного прошарку, який обслуговує опис сучасних банківських операцій. Цей прошарок не є повністю співставним ані з економічною, ані з комп'ютерною термінологією, а являє новостворену розвитком техніки сферу, що обслуговує функціонування банків на сучасному етапі.

Стан якості перекладу у вказаній сфері, так само як в окремо взятих галузях банківської справи та інформаційних технологій, знаходиться у постійному русі. Становлення термінологічної бази в ній великою мірою підпорядковано становленню термінів у базових галузях. Тим не менш термінологічний прошарок, який утворився в останні два десятиріччя, має і свої особливості. Наприклад, тема «Ідентифікація особистості» базується на термінології біометрики та оптики, а «Банківська документація» – на термінології фінансових звітів в електронному вигляді.

Практика перекладу банківської документації також показує, що зазвичай переклади виконуються банківськими службовцями, які не мають лінгвістичної освіти, й існуючі документи та рекламні проспекти потребують корекції як щодо термінології, так і стилістики викладу. Саме тому надані у посібнику практичні вправи та двомовні тексти мають підготувати перекладача до якісного перекладу.

Відомо, що для ефективного навчання перекладу треба озброїти студента не тільки необхідною термінологією, але і фоновими знаннями у певній галузі. Крім того, якість засвоєння перекладацьких навичок досягається методичною правильністю чергування різноманітних вправ – від найпростіших, що містять окремі слова та словосполучення, до синтагм та текстів, орієнтованих на стилістичну досконалість перекладу.

Оскільки посібник призначений як для користування в аудиторії, так і для самостійної роботи студента, для зручності він забезпечений англо-українським глосарієм у кінці книги. Важливим фактором для самоперевірки під час самостійної роботи є також наявність ключів для деяких вправ, які одночасно служать додатковими вправами для тренування автоматичних навичок перекладу.

Для забезпечення фонових знань матеріал, що надається, знайомить читача з основними напрямками банківських інформаційних технологій, а саме:

- інтернет-банкінг і його підвиди;
- банкінг за допомогою мобільних телефонів;
- функціонування кол-центрів (або центрів дозвонювання);
- ризики у сфері інтернет-банкінгу;

– інноваційні технологій у банкінгу для клієнта;
– кібер-злочини;
– банківські інформаційні системи.

Текстовий матеріал дає поняття банківських інформаційних технологій і одночасно знайомить зі специфічною для цієї сфери термінологією.

Структура кожного модуля створює умови для засвоєння термінології та розвитку перекладацьких навичок і є уніфікованою для всього навчального посібника:

– вступ до певної теми у вигляді запитань;
– оригінальний текст;
– знаходження українських відповідників позначеної у тексті термінології;
– різноманітні вправи на підставлення у пропуски окремих синтагм;
– створення міні-глосарію для цього модуля, і, нарешті,
– текст-компресія та його переклад на українську мову.

Окрім модулів з описаними вправами, книга включає зразки деяких банківських документів з описом українською мовою та термінологічний англо-український та українсько-англійський словник.

У кожному модулі є лексична вправа “Match”, тобто співставлення англійського та українського варіантів активної лексики. Вона позначена зірочкою і має ключі, розміщені у кінці навчального посібника.

Посібник пройшов апробацію у навчальному процесі на спеціальності «Переклад» за спеціалізацією «Науково-технічний переклад» у 2010–2012 навчальних роках у Національному технічному університеті «Харківський політехнічний інститут» у вигляді електронної версії.

Призначений для широкого кола користувачів, студентів спеціальностей «Переклад» та «Германські мови», усних та письмових перекладачів-практиків та банківських службовців.

Module 1. Call-centers

Ex 1.1. Pre-reading: answer the questions:

1. Have you ever used call center support?
2. What skills do you think should call center managers have?

Ex 1.2. Read the text and translate

Call Centers Make or Break Relationships

It's fair to say that most **high-ranking bank executives** spend little time considering how their call center operation affects their institution's overall performance. That's a big mistake, because service centers have become a crucial arena for managing customers' overall experience. Those few minutes on the phone can literally make or break your bank's relationship with its customers. Managed properly, the exchange can win a lifetime of **customer loyalty**, as well as boost customer profitability. Handled poorly, the exchange can **alienate** customers forever.

The goal for any call center operation should be to achieve first-call resolution of any customer inquiry. Once they pick up a call, service agents have essentially one chance to get it right. For the bank, there is an additional **agenda**: successfully cross-selling another of the bank's products or services to make the individual customer more profitable.

Toward these goals, we have identified several best practices that issuing banks can adopt to ensure that **interactions** between their cardholders and service agents are perceived as positive client experiences. These include properly training call center staffers across the entire transaction cycle; providing them with adequate decision support technology (DST); cultivating a deeper understanding of customer demographics so you can anticipate their changing needs; closely managing all call centers facilities as if they were internal operations; and lastly, linking overall call center performance to the appropriate metrics. Properly executed, these techniques can boost the first-call effectiveness of call center operations-and thereby enhance the profitability of the bank as a whole.

Training service agents to handle a wide variety of tasks is vital to achieving first-call resolution. For example, call center performance starts at the acquisition

stage. When a new cardholder establishes initial contact with a call center, the agent must function as both **fraud detector** and salesperson. In the former role, he must ask the right questions to ensure authentication and preserve the security of the customer's information. In the latter role, he must be able to persuasively offer the cardholder **ancillary** products. And in some cases, the agent must function as a high-level **credit evaluator**, determining what credit level the applicant should receive. These multiple responsibilities cannot be met without intensive training, frequent follow-up, and refresher courses geared to current goals. Different skill sets are required when handling established customers. Issuers are now capitalizing on the opportunities that incoming calls provide service agents to introduce and sell new products, increase line balances and offer balance transfers. Training must focus on making the most of these opportunities.

One of the easiest ways to **frustrate** customers and drive them away is to require them to repeat the same personal information ad nauseam to a succession of service reps. So, institutions should also invest in appropriate DST that will efficiently answer, direct, and segment incoming customer inquiries.

Customer telephone integration (CTI) and customer relationship management (CRM) applications place valid, comprehensive customer information before the customer service agent instantly, so he or she can respond quickly to any customer inquiry. Furthermore, call center representatives should have access to all bank information and details at the customer level and be able to confirm specific account-level details so that incoming callers only have to identify themselves and verify their identity once.

When it comes to getting the most out of the customer interaction, there's no substitute for thoroughly knowing your customer base-and how it is changing over time. Many of the questions you should ask yourself about your customers are elementary, such as what languages are spoken where your customers reside?

Others are not so obvious. For example, how are the financial needs of various customer segments changing? Has a previously low-income rural area started to attract wealthy retirees with higher **discretionary** income? Indications of such a local demographic shift can be gleaned from outside sources such as government income tables, increases in local property tax rates and assessments, credit bureau preference tables, or from internal bank sources. Combining these sources of outside information with your bank's internal analytical tools should enable you to spot such demographic changes early, and modify bank strategies and policies accordingly.

This requires banks to manage their call centers closely. Unfortunately, many banks have an "offshore means out of mind" attitude when it comes to outsourced call center operations, taking a hands-off stance toward their day-to-day management. Too often the ratio of supervisors-to-staff at these facilities is low, and performance incentives are not focused on how well customer issues are resolved. In addition, some off-shore providers serve a variety of corporate clients out of the same facility, in some cases mixing customers with different service goals. This can create difficulties for supervisors, who must attempt to manage their staffs to differing

quality standards. Forward-thinking issuers are realizing that offshore call centers should be managed no differently than those they operate at home.

Call center performance also needs to be **evaluated** using the correct metrics. Many call center operations were formerly evaluated upon a single metric, namely, "How much volume can we push through?" Banks have recently become **savvier**. While no single metric prevails-10 issuers might embrace 10 different metrics for profitability-issuers nowadays are more likely to evaluate their call centers' performance on the cost of the agent pool versus its efficiency in resolving customer issues and collecting money.

A thorough diagnostic, **benchmarking** the issuer against peers, will identify ways to improve performance. Such an effort should have two **focal points**. The first is call center operations, including management strategy, **inbound** call management, capacity planning, performance management, management information systems (MIS) and customer satisfaction. The second focus is employee management and development, including hiring and **retention**, compensation, and development.

Ex 1.3. Answer the questions:

1. What is the biggest mistake of high-ranking bank executives?
2. What is the goal of any call center operation?
3. What are the best practices that issuing banks can adopt?
4. What are the two roles that call-center agent should act?
5. Why is first-call resolution so vital?
6. What are the elementary questions a call-center agent should ask first?
7. What are the focal points to improve call-center performance?

Ex 1.4. Match the Ukrainian translations to the English phrases:

a) high-ranking bank executives	1) кредитний експерт
b) customer loyalty	2) відлякувати
c) alienate	3) основні напрямки (пункти)
d) agenda	4) порівняльний аналіз
e) interactions	5) високопоставлене керівництво банка
f) fraud detector	6) утримання
g) ancillary	7) лояльність клієнтів
h) credit evaluator	8) вхідний виклик
i) frustrate	9) програма (на день)
j) discretionary income	10) розчарувати
k) evaluate	11) детектор шахрайства
l) savvier	12) частина особистого доходу, що залишається після задоволення основних потреб
m) benchmarking	13) додатковий
n) focal points	14) більш досвідчений
o) inbound call	15) взаємодії
p) retention	16) оцінювати

Ex 1.5. Complete the following sentences with the words in the box

relationship, customer loyalty, profitability, agenda; resolution, frustrate, evaluated, benchmarking

1. Those few minutes on the phone can literally make or break your bank's …….. with its customers.
2. Managed properly, the exchange can win a lifetime of ……., as well as boost customer …….
3. For the bank, there is an additional …….: successfully cross-selling another of the bank's products or services to make the individual customer more profitable.
4. Training service agents to handle a wide variety of tasks is vital to achieving first-call ……..
5. One of the easiest ways to …… customers and drive them away is to require them to repeat the same personal information ad nauseam to a succession of service reps.
6. Call center performance also needs to be …… using the correct metrics.
7. A thorough diagnostic, …… the issuer against peers, will identify ways to improve performance.

Ex 1.6. Insert the prepositions

with, of, to, in, for

1. ….. the bank, there is an additional agenda.
2. ….. the former role, he must ask the right questions to ensure authentication and preserve the security ….. the customer's information.
3. Training service agents to handle a wide variety ….. tasks is vital to achieving first-call resolution.
4. When it comes ….. getting the most out of the customer interaction, there's no substitute for thoroughly knowing your customer base-and how it is changing over time.
5. Combining these sources of outside information ….. your bank's internal analytical tools should enable you to spot such demographic changes early, and modify bank strategies and policies accordingly.

Ex 1.7. Here are the answers. Work out the questions

1. The goal for any call center operation should be to achieve first-call resolution of any customer inquiry.
2. Training service agents to handle a wide variety of tasks is vital to achieving first-call resolution.
3. When a new cardholder establishes initial contact with a call center, the agent must function as both fraud detector and salesperson.
4. One of the easiest ways to frustrate customers and drive them away is to require them to repeat the same personal information ad nauseam to a succession of service reps.

5. Call center performance also needs to be evaluated using the correct metrics.

6. A thorough diagnostic, benchmarking the issuer against peers, will identify ways to improve performance.

Ex 1.8. Match the term with its synonym

a) executive	1) managing
b) loyalty	2) interplay
c) to alienate	3) faith
d) agenda	4) dash
e) interaction	5) entering
f) ancillary	6) estimate
g) frustrate	7) additional
h) income	8) profit
i) to evaluate	9) smart
j) savvy	10) plan
k) focal	11) turn away
l) inbound	12) main

Ex 1.9. Give the English equivalent to the following:

Відлякувати; кредитний експерт; взаємодії; оцінювати; довіра; вхідний виклик; основний; високопоставлене керівництво банку; розчарувати; детектор шахрайства; рівень статків; утримання.

Ex 1.10. Give the Ukrainian equivalent to the following:

Ancillary; inbound; discretionary income; to evaluate; high-ranking bank executives; management strategy; retention; customer relationship management; profitability; capacity planning.

Ex 1.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Call Centers Make or Break Relationships	**Кол-центри будують або руйнують відносини**
It's fair to say that most high-ranking bank executives spend little time considering how their call center operation affects their institution's overall performance. That's a big mistake, because service centers have become a crucial arena for managing customers' overall experience. Those few minutes on the phone can literally	Справедливо було б сказати, що більшість високопоставлених банківських службовців витрачають замало часу для оцінювання своїх кол-центрів. Це велика помилка, тому що, використовуючи накопичений досвід, центри обслуговування стали основним місцем роботи з клієнтом. Ці кілька хвилин спілкування по

make or break your bank's relationship with its customers. Managed properly, the exchange can win a lifetime of customer loyalty, as well as boost customer profitability. Handled poorly, the exchange can alienate customers forever.	телефону мають змогу в буквальному розумінні започаткувати або зруйнувати відносини вашого банку із замовником. Побудоване належним чином спілкування з клієнтом має можливість заслужити його довічну довіру до банку і таким чином різко збільшити прибуток, тоді як некоректне спілкування відлякує клієнта назавжди.
The goal for any call center operation should be to achieve first-call resolution of any customer inquiry. Once they pick up a call, service agents have essentially one chance to get it right. For the bank, there is an additional agenda: successfully cross-selling another of the bank's products or services to make the individual customer more profitable.	Метою будь-якого кол-центру має бути вирішення проблеми клієнта після першого дзвінка. Коли виклик одержано, агенти сервісного центру, по суті, мають лише один шанс прийняти правильне рішення. Стосовно банку існує також додаткова програма, яка полягає в успішному здійсненні перехресних продаж інших банківських продуктів і послуг для одержання більшого прибутку з кожного окремого клієнта.
Toward these goals, we have identified several best practices that issuing banks can adopt to ensure that interactions between their cardholders and service agents are perceived as positive client experiences. These include properly training call center staffers across the entire transaction cycle; providing them with adequate decision support technology (DST) and cultivating a deeper understanding of customer demographics so you can anticipate their changing needs.	Для досягнення цих цілей ми визначили низку максимально продуктивних методів, якими мають змогу скористатися емісійні банки, щоб переконатися, що взаємодія між користувачами карток і сервісними агентами сприймається клієнтами позитивно. Це включає належну підготовку співробітників кол-центру для здійснення всього циклу укладених угод, надання їм належні технології прийняття рішень (ТПР) та виховання у них глибокого розуміння демографії клієнтів для передбачення потреб, що змінюються.
Training service agents to handle a wide variety of tasks is vital to achieving first-call resolution. For example, call center performance starts at the acquisition stage.	Правильно виконані ці методи можуть різко підвищити ефективність першого дзвінка і таким чином у цілому підвищити прибуток банку.

When a new cardholder establishes initial contact with a call center, the agent must function as both fraud detector and salesperson. In the former role, he must ask the right questions to ensure authentication and preserve the security of the customer's information. In the latter role, he must be able to persuasively offer the cardholder ancillary products. And in some cases, the agent must function as a high-level credit evaluator, determining what credit level the applicant should receive.	Коли новий клієнт встановлює перший контакт з кол-центром, агент повинен діяти одночасно як детектор шахрайства і як продавець. В першій ролі він повинен ставити необхідні запитання, щоб переконатися у достовірності інформації і зберегти безпечність інформації клієнта. В другій ролі він повинен переконливо прорекламувати клієнту додаткові послуги. А в деяких випадках мусить також виконувати роль кредитного експерта високого рівня, щоб встановити, який рівень кредиту можна надати клієнту.
One of the easiest ways to frustrate customers and drive them away is to require them to repeat the same personal information ad nauseam to a succession of service reps. So, institutions should also invest in appropriate DST that will efficiently answer, direct, and segment incoming customer inquiries.	Один з найпростіших способів розчарувати клієнтів і віджахнути їх є настирність працівників сервісного центру, з якою вони повторюють одну і ту ж саму інформацію. Таким чином, банківські установи повинні робити інвестиції в системи підтримки прийняття рішень, які дозволяють ефективно відповідати на вхідні запити клієнтів.
Many of the questions you should ask yourself about your customers are elementary, such as what languages are spoken where your customers reside? Others are not so obvious. For example, how are the financial needs of various customer segments changing? Has a previously low-income rural area started to attract wealthy retirees with higher discretionary income? Indications of such a local demographic shift can be gleaned from outside sources such as government income tables, increases in local property tax rates and assessments, credit bureau preference tables, or from internal bank sources.	Значний обсяг інформації, яку ви повинні знати про клієнтів, є елементарним. Наприклад, на якій мові розмовляють у місцевості, де проживають клієнти. Інша інформація не є такою явною. Наприклад, яким чином змінюються фінансові потреби різних сегментів клієнтської бази. Чи стали сільські райони з низьким рівнем статків привабливими для пенсіонерів з більш високим рівнем статків. Інформацію про такі місцеві демографічні зрушення можна почерпнути із зовнішніх джерел, таких, як державні таблиці статків, дані про збільшення місцевого видатку на нерухомість і ставки видатків з таблиць кредитних бюро або з

Many call center operations were formerly evaluated upon a single metric, namely, "How much volume can we push through?" Banks have recently become savvier. While no single metric prevails-10 issuers might embrace 10 different metrics for profitability-issuers nowadays are more likely to evaluate their call centers' performance on the cost of the agent pool versus its efficiency in resolving customer issues and collecting money.	внутрішніх джерел банку. Раніше більшість операцій кол-центрів оцінювалась за допомогою одного показника, а саме, «скільки ми можемо обслужити клієнтів». Останнім часом банки стали більш досвідченими, хоча жоден з методів не переважає: десять компаній можуть використовувати десять різних показників ефективності. Зараз компанії скоріш оцінюють продуктивність кол-центрів за співвідношенням витрат на утримання персоналу та їх ефективності в вирішенні питань клієнтів і зібраних грошей.
A thorough diagnostic, benchmarking the issuer against peers, will identify ways to improve performance. Such an effort should have two focal points. The first is call center operations, including management strategy, inbound call management, capacity planning, performance management, management information systems (MIS) and customer satisfaction. The second focus is employee management and development, including hiring and retention, compensation, and development.	Ретельний порівняльний аналіз показників відділу зі схожими відділами допоможе визначити шляхи покращення роботи підприємств. Такі зусилля повинні мати два напрямки. По-перше, це операції кол-центрів, які включають стратегії управління, керування потоками викликів, планування, системи управління (СУ) і задоволення клієнтів. Другим напрямком є керування персоналом і розвитком, в тому числі найм та утримання, компенсація і розвиток.

Module 2. Management Information System

Ex 2.1. Pre-reading: answer the questions:

1. Do you suppose that modern banking supervision is developed enough?
2. How does inner banking management affect common clients?

Ex 2.2. Read the text:

Management Information System

SIM-SPBI is an integrated information system that supports the functions **of banking supervision, examination** and control. In general the management information system for the banking sector is essentially a means of automating the functions of Bank Supervision and Examination, including the collection, calculation and presentation of data / information, it is also to create an integrated information center so that information is always available to support the roles of supervision, examination, research, control and development of the banking system. With available data on bank performance that is comprehensive, prompt and accurate, bank is confident to have the support needed for decision-making, and that the data can be used by other concerned parties in line with **existing procedures**.

The goals of application of the SIM-SPBI are:

To improve the effectiveness and efficiency of the bank supervision and examination system;

To bring about standardization in the implementation of the functions of bank supervision and examination;

To optimize the analysis of Bank Supervisors and Examiners of bank performance to improve the quality of bank supervision and examination;

To facilitate examination of the **audit trail** by the competent authorities;

To increase the security and integrity of bank data and information.

SIM-SPBI is expected to improve the integrity and competence of bank supervisors and examiners and **to upgrade the effectiveness** of bank supervision, which in its turn could create a sound banking system.

1. **Supervision Management Information System (SIMWAS)**: The SIMWAS information system was developed to improve the effectiveness and

efficiency of the Commercial Bank supervision system. By means of the SIMWAS, bank supervisors can optimize the analysis of bank performance, expedite the collection of data regarding bank finances, and increase the security and integrity of banking system data and information. The modules of the SIMWAS software application include, among others, the Bank Basic Data and Fit and Proper Test (FPT) modules. The FPT module provides complete information concerning the profiles of prospects and or management and controlling **shareholders** of a bank.

2. **Bank Investigation Information System (SIBADI)**: The SIBADI information system was developed to improve administrative discipline and **facilitate** ease of monitoring of the functions of investigation of **criminal acts in the banking system** by the Directorate of Banking System Investigation and Mediation (DIMP). The SIBADI system enables the monitoring of the progress of an investigation of a suspected criminal act perpetrated by a bank from the point a report of **infringement** is received (from a banking system supervision unit or the public), the schedule of the investigation, and the measures initiated until the final results of the investigation in question. The SIBADI information system is intended to automate the administrative activities of an investigation of a criminal act in the banking sector through the collection and presentation of data / information, and to create an integrated and readily available information center to support the functions of investigation of a criminal act in the banking system, as well as measures of **mediation** between a client and a bank.

3. **Data Mart**: The Data Mart software application provides information related to the institutionalization, ownership and management and operations and supervision strategy adopted by a bank, thus, the system is expected to optimize the information required for supervision and guided development of a bank.

Debitor Information System (SID)

SID is an information system designed to provide information regarding debtors, both individuals or businesses. The information is processed based on reporting institution of available funds received by bank from Reporters. SID was developed to assist with the following goals:

1. Internally:

– Bank supervision, and

– Stability of the financial system.

2. Externally:

With respect to credit providers, among other things:

– To assist the prompt process of analysis and decision-making regarding a credit **disbursement**;

– To reduce the dependency of a credit provider on conventional **collateral**. Credit providers can assess the credit record of a prospect debtor as a substitute / compliment to collateral.

With respect to credit recipients, among other things:

– To expedite the time required to obtain credit approval;

– New clients, particularly those classified as Small/Micro Businesses, can have wider access to credit providers, whereby their credibility is judged by their financial record rather than depending solely upon their ability to provide collateral.

Rural Bank Supervision Management Information System (SIMWAS BPR)

In an effort to improve the effectiveness of implementation of the functions of supervision, examination and research of rural bank, banks designed the Rural Bank Supervision Management Information System (SIMWAS BPR) which was implemented in July 2005. The SIMWAS BPR information system was created to improve the effectiveness and efficiency of the BPR supervision system. Using the SIMWAS BPR, BPR supervisors can optimize the analysis of the performance of a BPR, **expedite** access to information regarding the financial condition of BPR (including BPR Soundness rating), and increase the security and integrity of banking system data and information.

Ex 2.3. Answer the questions:

1. What is SIM-SPBI?
2. What are the goals of application of the SIM-SPBI?
3. What is SIM-SPBI expected to improve?
4. What is the goal of Supervision Management Information System development?
5. What does Data Mart software application provide?
6. What are the goals of Debitor Information System?
7. How can SIMWAS help supervisors?

Ex 2.4. Match the Ukrainian translations to the English phrases:

a) audit trail	1) майнова застава
b) shareholder	2) акціонер
c) facilitate	3) журнал контролю
d) disbursement	4) виплата
e) collateral	5) спрощувати
f) banking supervision	6) запровадити стандартизацію
g) examination	7) злочини у банківській системі
h) existing procedures	8) банківське спостереження
i) upgrade the effectiveness	9) скорити час
j) bring about standardization	10) фінансова довіра
k) criminal acts in the banking system	11) поточні операції
l) mediation	12) порушення
m) expedite the time	13) експертиза
n) infringement	14) посередництво
o) credibility	15) покращити безпеку

Ex 2.5. Complete the following sentences from the words in the box

efficiency, analysis, accurate, integrity, examination, ownership, prompt, investigation, integrated information system, improve.

1. SIM-SPBI is an ……. that supports the functions of banking supervision, …… and control.
2. With available data on bank performance that is comprehensive, …….. and ……., bank is confident to have the support needed for decision-making.
3. SIM-SPBI is expected to improve the …….. and competence of bank supervisors.
4. By means of the SIMWAS, bank supervisors can optimize the …….. of bank performance.
5. The SIBADI information system was developed to …… administrative discipline
6. The SIBADI system enables the monitoring of the progress of an …… of a suspected criminal act.
7. The Data Mart software application provides information related to the institutionalization, ……. and management.
8. The SIMWAS BPR information system was created to improve the effectiveness and ……. of the BPR supervision system.

Ex 2.6. Insert the prepositions

with, from, for, to, of, by

1. In general the management information system …. the banking sector is essentially a means …. automating the functions of Bank Supervision and Examination.
2. Bank is confident …. have the support needed for decision-making.
3. …. means of the SIMWAS, bank supervisors can optimize the analysis of bank performance.
4. The information is processed based on reporting institution of available funds received by bank …. Reporters.
5. SID was developed to assist …. the following goals…

Ex 2.7. Here are the answers. Work out the questions.

1. In general the management information system for the banking sector is essentially a means of automating the functions of Bank Supervision and Examination.
2. With available data on bank performance that is comprehensive, prompt and accurate, bank is confident to have the support needed for decision-making, and that the data can be used by other concerned parties in line with existing procedures.
3. The goals of application of the SIM-SPBI are:

– To improve the effectiveness and efficiency of the bank supervision and examination system;

– To bring about standardization in the implementation of the functions of bank supervision and examination;

– To optimize the analysis of Bank Supervisors and Examiners of bank performance to improve the quality of bank supervision and examination;

4. By means of the SIMWAS, bank supervisors can optimize the analysis of bank performance, expedite the collection of data regarding bank finances, and increase the security and integrity of banking system data and information.

5. The Data Mart software application provides information related to the institutionalization, ownership and management.

6. Supervisors can optimize the analysis of the performance of a BPR, expedite access to information regarding the financial condition of BPR (including BPR Soundness rating), and increase the security and integrity of banking system data and information, using the SIMWAS BPR.

Ex 2.8. Match the term with its definition

a) disbursement	1) payment
b) examination	2) attempt to bring to agreement
c) to upgrade	3) make happen faster
d) standardization	4) test
e) mediation	5) breach
f) to expedite	6) improve
g) infringement	7) uniformity

Ex 2.9. Translate into English

Майнова застава; виплата; неускладнений; журнал контролю; запровадити стандартизацію; посередництво; скорити; фінансова довіра; поточні операції; банківське спостереження.

Ex 2.10. Translate into Ukrainian

Credibility; to facilitate; collateral; banking supervision; existing procedures; to bring about standardization; examination; audit trail; mediation; to expedite the time; infringement; disbursement.

Ex 2.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English translation by covering one part of the matching texts. If necessary, consult the covered text.

Management Information System	**Інформаційна система управління**
SIM-SPBI is an integrated information system that supports the functions of banking **supervision**, examination and control. In general the management information system for the	SIM-SPBI – це інтегрована інформаційна система, яка підтримує функції банківського управління, експертизи і контролю. Загалом управлінська інформаційна система

banking sector is essentially a means of automating the functions of Bank Supervision and Examination, including the collection, calculation and presentation of data / information, it is also to create an integrated information center so that information is always available to support the roles of supervision, examination, research, control and development of the banking system. With available data on bank performance that is comprehensive, prompt and accurate, bank is confident to have the support needed for decision-making, and that the data can be used by other concerned parties in line with existing procedures.	для банківського сектора – це, головним чином, засіб автоматизації функцій банківського нагляду та експертизи, включаючи збір, обчислення і надання даних/інформації, який також служить для створення інтегрованого інформаційного центру, де інформація була б завжди доступною, щоб підтримати функції спостереження, експертизи, дослідження, контролю і розвитку банківської системи. За наявності доступних даних щодо дієздатності банку, які є **усебічними**, швидкими і точними, банк упевнений в **наявності** підтримки, необхідної для ухвалення рішень, а також у тому, що дані можуть використовуватися іншими зацікавленими сторонами паралельно з поточними операціями.
The goals of application of the SIM-SPBI are: • To improve the effectiveness and efficiency of the bank supervision and examination system; • To bring about standardization in the implementation of the functions of bank supervision and examination; • To facilitate examination of the audit trail by the competent authorities; • To increase the security and integrity of bank data and information. SIM-SPBI is expected to improve the integrity and competence of bank supervisors and examiners and to upgrade the effectiveness of bank supervision, which in its turn could create a sound banking system.	Цілі застосування SIM - SPBI: • підвищення рівня ефективності і дієвості системи банківського нагляду та експертизи; • запровадження стандартизації у впровадженні функцій банківського нагляду та експертизи; • полегшення перевірки контрольного журналу компетентними органами; • посилення безпеки і цілісності банківських даних та інформації. SIM-SPBI, як очікують, поліпшить чесність і компетентність банківських спостерігачів і ревізорів та покращить ефективність банківського нагляду, який, у свою чергу, може створити надійну банківську систему.

1. Supervision Management Information System (SIMWAS): The SIMWAS information system was developed to improve the effectiveness and efficiency of the Commercial Bank supervision system. By means of the SIMWAS, bank supervisors can optimize the analysis of bank performance, expedite the collection of data regarding bank finances (including Bank Soundness rating), and increase the security and integrity of banking system data and information.	**1. Управлінська Інформаційна система спостереження (SIMWAS)**: інформаційна система SIMWAS була розроблена, щоб покращити ефективність і дієвість системи спостереження комерційного банку. За допомогою SIMWAS банківські спостерігачі можуть оптимізувати аналіз роботи банку, прискорити збір даних про фінанси банку (включаючи рівень його надійності), покращити безпеку і надійність даних та інформації банківської системи.
2. Bank Investigation Information System (SIBADI): The SIBADI information system was developed to improve administrative discipline and facilitate ease of monitoring of the functions of investigation of criminal acts in the banking system. The SIBADI system enables the monitoring of the progress of an investigation of a suspected criminal act perpetrated by a bank from the point a report of infringement is received. The SIBADI information system is intended to support the functions of investigation of a criminal act in the banking system, as well as measures of mediation between a client and a bank.	**2. Інформаційна система банка (SIBADI):** інформаційна система SIBADI була розроблена для підвищення адміністративної дисципліни і полегшення контролю функцій дослідження злочинів у банківській системі. Система SIBADI дозволяє контролювати прогрес **дослідження** підозрюваного злочину, здійсненого стосовно банку, починаючи з моменту повідомлення про порушення. Інформаційна система SIBADI призначена для підтримки функції як **дослідження** злочину у банківській системі, так і заходів посередництва між клієнтом і банком.
3. Data Mart: The Data Mart software application provides information related to the institutionalization, ownership and management and operations and supervision strategy adopted by a bank, thus, the system is expected to optimize the information required for supervision and guided development of a bank.	3. **База даних:** надає інформацію, пов'язану з інституціоналізацією, власністю, управлінням, операціями і стратегією спостереження, прийнятою банком. Таким чином система, як очікують, оптимізує інформацію, затребувану для спостереження і керованого розвитку банку.

Debitor Information System (SID)	**Інформаційна система боржника (SID)**
SID was developed to assist with the following goals: With respect to credit providers, among other things: • To assist the **prompt** process of analysis and decision-making regarding a credit disbursement; • To reduce the dependency of a credit provider on conventional collateral. Credit providers can assess the credit record of a prospect debtor as a substitute/compliment to collateral. With respect to credit recipients, among other things: • To expedite the time required to obtain credit approval; • New clients, particularly those classified as Small/Micro Businesses, can have wider access to credit providers, whereby their credibility is judged by their financial record rather than depending solely upon their ability to provide collateral.	SID був розроблений для допомоги з такими цілями: Стосовно кредитних організацій серед інших цілей: • з метою скорення процесу аналізу та ухвалення рішень щодо виплати кредиту; • зменшення залежності кредитних організацій від майнової застави. Кредитні організації можуть оцінити кредитну історію ймовірного боржника як заміну/додаток до майнової застави. Стосовно одержувачів кредиту, серед інших цілей: • зменшення часу, потрібного для отримання схвалення кредиту; • у нових клієнтів, особливо класифікованих як маленькі/мікро фірми, може бути ширший доступ до можливостей отримання кредиту, за допомогою чого довіра до них оцінюється за їх фінансовим звітом замість того, щоб залежати виключно від їх здатності забезпечити майнову заставу.

Module 3. Online Banking: Information Security vs. Hackers

Ex 3.1. Pre-reading: answer the questions:

1. Have you ever carried out any kind of banking transactions online?
2. Do you know any security measures the financial institutions take to protect the information?

Ex 3.2. Read the text and translate

Online Banking: Information Security vs. Hackers

Billions of financial data transactions occur online every day of the year 24 hours a day 7 days a week and bank cybercrimes take place every day when bank information **is compromised**. Skilled criminal hackers can manipulate a financial institution's online information system, **spread malicious bank Trojan viruses** that **allow remote access to** a computer, **corrupt data,** and **impede** the quality of an information system's performance. If sensitive information is not better protected, **cyber-thieves** will continue **to illegally access** online financial accounts to steal trillions of dollars plus **sensitive customer information** globally. Audit of bank information technology systems, ethics and policy requirements for bank information security systems, awareness of risk potential, continuity of financial institution information systems all should be high on the list of **federal & state regulators** and banking board of director's agenda meetings. One major real world cybercrime directed at any specific financial institution can severely **take down a domestic and global financial network.**

Banks and Savings & Loans is identified as financial institutions and both are **custodians of** not only their customer's money, but even more so a financial institution is responsible for their customer's personal and legacy data. Examples of information that financial institutions are the custodian of records for their commercial and personal banking customers is: day-to-day transactions including

deposits, **withdrawals**, **balance amount**, social security number, birth date**, loan information**, partnership agreements related to a loan**, year-to-date statements** and a host of other extremely sensitive financial information. All the above mentioned records, transactions and sensitive information are events that occur online usually more than 50 percent of the time.

Cyber crooks, network hackers, cyber pirates, internet thieves is an emerging crime category of criminals and threat to online banking information security systems. The efforts used to **hi-jack** financial institutions was Banking Trojans that **piggy-back** legitimate customer bank accounts to steal passwords, fraudulent wire transfers, and hackers working from the inside to compromise the information security system of an financial institution, in other words; **an inside job.**

Ex 3.3. Answer the questions:

1. Who is responsible for audition of bank information technology systems?
2. Who are the custodians of customer's money responsible for their customer's personal and legacy data?
3. What personal data do the financial institutions keep?
4. What means did cyber crooks use to hi-jack financial institutions?

Ex 3.4. Match the Ukrainian translations to the English phrases

a) financial data transactions	1) грабувати
b) cyber crimes	2) особиста інформація клієнта
c) compromise	3) державна та світова фінансова мережа
d) allow remote access to	4) банківські та кредитні установи
e) impede	5) правонаступник
f) cyber-thieves	6) транзакції з фінансовими даними
g) illegally access	7) кібер-злочин
h) sensitive customer information	8) перешкоджати
i) take down	9) незаконно проникати
j) a domestic and global financial network.	10) руйнувати
k) Banks and Savings & Loans	11) наражати на небезпеку
l) custodian	12) кібер-злочинець
m) legacy data	13) комбінований, додатковий
n) hi-jack	14) дозволяти дистанційний доступ
o) withdrawals	15) зняття грошей з рахунку
p) cyber crooks	16) дані про спадщину
q) piggy-back	17) кібер-аферисти

Ex 3.5. Complete the following sentences with the words from the box

allow remote access; compromise ; corrupt; custodian; federal & state regulators; loan information ;impede; cyber crooks, network hackers, cyber pirates; to illegally access; withdrawals; year-to-date statements

1. Audit of bank information technology systems, ethics and policy requirements for bank information security systems, awareness of risk potential, continuity of financial institution information systems all should be high on the list of …….and banking board of director's agenda meetings.

2. Hackers working from the inside ……..the information security system of a financial institution.

3. ……..is an emerging crime category of criminals and threat to online banking information security systems.

4. Trojan viruses that ……to a computer, …….data, and…… the quality of an information system's performance.

5. If sensitive information is not better protected, cyber-thieves will continue …… online financial accounts.

6. Examples of information that financial institutions are the ……..of records for their commercial and personal banking customers is: day-to-day transactions including deposits, ……., balance amount, social security number, birth date, ……., partnership agreements related to a loan, …….and a host of other extremely sensitive financial information.

Ex 3.6. Match the term with its definition

a) year-to-date statement b) cyber crimes c) withdrawal d) inside job e) cyber crooks f) Federal & state regulators g) to impede h) to piggy-back	1) a crime committed online 2) to hinder 3) computer professionals committing different kinds of online crimes 4) organs which audit bank information technology systems 5) the process of taking money off 6) a word connected with the situation when a cyber-crook penetrates into a sensitive bank information to spread viruses and use a customer's account 7) a type of a crime with the participation of employee of the financial institution 8) the system of signs, grouped into a summary list, reflecting the assets and sources of formation in monetary units for the beginning of the year

Ex 3.7. Insert the prepositions

to, of, for, on, at, from

1. Skilled criminal hackers can spread malicious bank Trojan viruses that allow remote access ….. a computer, corrupt data, and impede the quality … an information system's performance.

2. Audit of bank information technology systems, ethics and policy requirements … bank information security systems, awareness … risk potential, continuity of financial institution information systems all should be high … the list of federal & state regulators and banking board of director's agenda meetings.

3. One major real world cybercrime directed … any specific financial institution can severely take down a domestic and global financial network..

4. Financial institutions are custodians …not only their customer's money, but even more so a financial institution is responsible …. their customer's personal and legacy data.

5. The efforts used to hi-jack financial institutions was Banking Trojans that piggy-back legitimate customer bank accounts to steal passwords, fraudulent wire transfers, and hackers working ….. the inside to compromise the information security system of a financial institution.

Ex 3.8. Translate into Ukrainian

Financial data transaction; piggy-back; cyber crimes; cyber crooks; to hi-jack; compromise; withdrawal; allow remote access to; legacy data; a domestic and global financial network; impede; to be a custodian of; Banks and Savings & Loans; take down; cyber-thieves; sensitive customer information; to illegally access; year-to-date statement.

Ex 3.9. Translate into English

Грабувати; кібер-аферисти; особиста інформація клієнта; проникати; державна та світова фінансова мережа; зняття грошей з рахунку; банківські та кредитні установи; відкривати дистанційний доступ до; успадковані дані; зберігати; транзакції фінансових даних; кібер-злочин; наражати на небезпеку; перешкоджати; руйнувати; незаконно проникати.

Ex 3.10. Translate the sentences into Ukrainian

1. Banks and Savings & Loans is identified as financial institutions and both are custodians of not only their customer's money, but even more so a financial institution is responsible for their customer's personal and legacy data.

2. Cyber crooks, network hackers, cyber pirates, internet thieves is an emerging crime category of criminals and threat to online banking information security systems.

3. Skilled criminal hackers can manipulate a financial institution's online information system, spread malicious bank Trojan viruses that allow remote access to a computer, corrupt data, and impede the quality of an information system's performance.

4. If sensitive information is not better protected, cyber-thieves will continue to illegally access online financial accounts to steal trillions of dollars plus sensitive customer information globally.

5. The efforts used to hi-jack financial institutions was Banking Trojans that piggy-back legitimate customer bank accounts.

Ex 3.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Online Banking: Information Security vs. Hackers	**Захист банківської інформації від хакерів у реальному часі**
Billions of **financial data transactions** as well as bank **cybercrimes** occur online every day of the year 24 hours a day 7 days a week when bank information is **compromised.** Skilled criminal hackers can manipulate a financial institution's online information system, spread malicious bank Trojan viruses that **allow remote access** to a computer, corrupt data, and **impede** the quality of an information system's performance. It is necessary to prevent **cyber-thieves to illegally access** online financial accounts to steal trillions of dollars plus **sensitive customer information** globally. **Federal & state regulators** ought to audit bank information technology systems. One major real world cyber crime can severely **take down a domestic and global financial network.**	Кожні 24 години 7 днів на тиждень мільярди як транзакцій фінансових даних, так і кібер-злочинів здійснюється онлайн, коли банківська інформація наражається на небезпеку. Професійні злочинці – хакери можуть маніпулювати інформаційною онлайн системою фінансової установи, поширювати небезпечні банківські троянські віруси, що відкривають дистанційний доступ до комп'ютера, спотворюють дані, а також перешкоджають якісній роботі інформаційної системи. Необхідно перешкодити кібер-злодіям незаконно проникати онлайн до фінансових рахунків, красти трильйони доларів й особисту інформацію клієнтів по всьому світу. Державні та регіональні регулятивні органи повинні перевіряти системи інформаційних технологій банків. Один серйозний кібер-злочин в реальному світі може жорстоко зруйнувати державну і світову фінансову систему.
Banks and Savings & Loans (i.e. financial institutions) are **custodians** of not only their customer's money but they are responsible for their customer's personal and **legacy data** as well. For instance- day-to-day transactions including deposits, **withdrawals, balance amount,** social security number, birth date,	Банки і кредитні установи (тобто фінансові інститути) зберігають не тільки гроші клієнта, але й несуть відповідальність за особисті та успадковані дані. Наприклад: щоденні транзакції, такі як депозити, зняття грошей з рахунку, залишок суми на рахунку, номер соціального страхування, дата народження, інформація про позику, угоди про співпрацю стосовно позики, баланс на

loan information, partnership agreements related to a loan, **year-to-date statements** and a host of other extremely sensitive financial information. The events mentioned above occur online usually more than 50 percent of the time.	початку року і багато іншої надзвичайно делікатної фінансової інформації. Операції вказані вище, більше ніж 50 % часу відбуваються онлайн.
Cyber crooks, network hackers**,** cyber pirates, internet thieves tried **to hi-jack** financial institutions by means of Banking Trojans that **piggy-back** legitimate customer bank accounts and **inside job** to compromise the information security system.	Кібер-аферисти, мережеві хакери, кібер-пірати, інтернет-крадії намагалися грабувати фінансові установи шляхом впровадження банківського троянського вірусу, який проникає до справжніх банківських рахунків клієнта, а також за допомогою банківських працівників з метою поставити під загрозу інформаційну безпеку системи.

Module 4. Trends in mobile banking

Ex. 4.1. Pre-reading: answer the questions:

1. Name as many activities of mobile banking as you can.
2. What do you think mobile banking stands for?

Ex. 4.2. Read the text below and answer the questions:

Trends in mobile banking

The advent of the Internet has revolutionized the way the financial services industry **conducts business**, empowering organizations with new business models and new ways to offer 24x7 **accessibility to their customers**.

The ability to offer financial transactions online has also created new players in the financial services industry, such as **online banks**, **online brokers** and wealth managers who offer personalized services, although such players still account for a tiny percentage of the industry.

Over the last few years, the mobile and **wireless market** has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to the GSM Association and Ovum, the number of **mobile subscribers** exceeded 2 billion in September 2005, and now exceeds 2.5 billion

According to a study by financial consultancy Client, 35 % of **online banking households** will be using mobile banking by 2010, up from less than 1 % today. Upwards of 70 % of bank center call volume is projected to come from mobile phones. Mobile banking will eventually allow users to make payments at **the physical point of sale**. "**Mobile contactless payments**" will make up 10 % of the **contactless market**.

Many believe that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries, where mobile infrastructure is comparatively better than the **fixed-line infrastructure**, and in European countries, where mobile phone penetration is very high (at least 80 % of consumers use a mobile phone), mobile banking is likely to appeal even more.

This opens up huge markets for financial institutions interested in **offering value added services**. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while travelling, **receiving online updates** of stock price or even **performing stock trading** while being stuck in traffic.

Mobile devices, especially smartphones, are the most promising way to reach the masses and to create "stickiness" among current customers, due to their ability to provide services anytime, anywhere, high rate of penetration and potential to grow.

In the past decades, banks across the globe have invested billions of dollars to build **sophisticated internet banking capabilities**. As the trend is shifting to mobile banking, there is a challenge for CIOs and CTOs of these banks to decide on how to **leverage their investment** in internet banking and offer mobile banking, in the shortest possible time.

The proliferation of the 3G (third generation of wireless) and widespread implementation expected for the beginning of the century will generate the development of more sophisticated services such as multimedia and links to **m-commerce services**.

Ex. 4.3. Answer the questions:

1. What did the advent of the Internet change in business sphere?
2. What does the study by financial consultancy Celent state?
3. What advantages does mobile technology give to the banks?
4. When is the proliferation of the 3G expected?
5. What advantages can 3G give?

Ex. 4.4. Match the Ukrainian translations to the English phrases:

a) mobile banking	1) грошові перекази
b) conduct business	2) родини – користувачі онлайн-банкінгу
c) accessibility to customers	3) пропозиція послуг із доданою вартістю
d) offer financial transactions online	4) безконтактний ринок
e) online banks	5) високотехнологічні можливості інтернет-банкінгу
f) online brokers	6) пропонувати фінансові операції в режимі онлайн
g) wireless market	7) мобільний банкінг
h) mobile subscribers	8) доступ для клієнтів
i) online banking households	9) інфраструктура провідних ліній
j) physical point of sale	10) залучення інвестицій
k) mobile contactless payments	11) онлайн-банки
l) contactless market	12) отримувати онлайн-оновлення
m) fixed-line infrastructure	13) вести бізнес
n) offer value added services	14) послуги мобільної комерції
o) funds transfer	15) виконання торгівельних операцій з
p) receive online updates	

q) perform stock trading r) sophisticated internet banking capabilities s) leverage of investment t) m-commerce services	акціями (цінними паперами) 16) онлайн-брокери 17) абоненти мобільного зв'язку 18) мобільні безконтактні платежі 19) ринок безпровідного зв'язку 20) фізичний пункт продажу (пристрій)

Ex 4.5. Complete the following sentences from the words in the box

leverage, investment, wireless market, online banking households, online brokers, wealth managers, smartphones, proliferation, online banks

1. The ability to offer financial transactions online has also created new players in the financial services industry, such as ……., …….. and …….
2. Over the last few years, the mobile and ……. has been one of the fastest growing markets in the world.
3. 35 % of …….. will be using mobile banking by 2010.
4. Mobile devices, especially ……, are the most promising way to reach the masses.
5. There is a challenge for the banks to decide on how to …….. their…….. in internet banking.
6. The …….. of the 3G is expected for the beginning of the century.

Ex 4.6. Insert the prepositions

at, of, to, for, with

1. The advent …. the Internet has revolutionized the way the financial services industry conducts business.
2. The ability …. offer financial transactions online has also created new players in the financial services industry.
3. Upwards …. 70 % of bank center call volume is projected …. come from mobile phones.
4. …. mobile technology, banks can offer a wide range of services to their customers.
5. Mobile banking will eventually allow users to make payments …. the physical point of sale.
6. The proliferation of the 3G is expected …. the beginning of the century.

Ex 4.7. Here are the answers. Work out the questions

1. Online banks, online brokers and wealth managers are the new players in the financial services industry.
2. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while travelling, receiving online updates of stock price or even performing stock trading while being stuck in traffic.

3. Mobile devices, especially smartphones, are the most promising way to reach the masses and to create “stickiness” among current customers, due to their ability to provide services anytime, anywhere, high rate of penetration and potential to grow.

4. The proliferation of the 3G (third generation of wireless) and widespread implementation expected for the beginning of the century will generate the development of more sophisticated services such as multimedia and links to m-commerce services.

Ex 4.8. Find the synonyms

a) subscriber	1) client
b) wireless	2) deal
c) leverage	3) signer
d) customer	4) expense
e) conduct	5) contactless
f) fund	6) advantage
g) investment	7) reserve
h) value	8) price
i) transfer	9) relocation

Ex 4.9. Translate into English

Грошові перекази; родини – користувачі онлайн-банкінгу; безконтактний ринок; складні можливості інтернет-банкінгу; мобільний банкінг; доступ для клієнтів; інфраструктура провідних ліній; залучення інвестицій; онлайн-банки; вести бізнес; сервіси мобільної комерції; онлайн-брокери; абоненти мобільного зв’язку; мобільні безконтактні платежі; фізичний пункт продажу.

Ex 4.10. Translate into Ukrainian

Conduct business; accessibility; wireless; subscribers; online banking households; physical point of sale; contactless; payments; fixed-line; value added services; funds; online updates; stock trading; sophisticated; leverage; investment; m-commerce services.

Ex 4.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Trends in mobile banking	**Тенденції у сфері мобільного банкінгу**
The advent of the Internet has revolutionized the way the financial services industry conducts business, empowering organizations with new business models and new ways to offer	Поява інтернету відкрила новий шлях для фінансових послуг у бізнесі, розширюючи можливості за рахунок нових бізнес-технологій і нових можливостей доступу у щоденному

24x7 accessibility to their customers.	цілодобовому режимі 24×7 своїм клієнтам.
The ability to offer financial transactions online has also created new players in the financial services industry, such as online banks, online brokers and wealth managers who offer personalized services.	Здатність запропонувати фінансові операції онлайн також створила нових гравців в індустрії фінансових послуг, таких як онлайн-банки, онлайнові брокери і менеджери коштів, що пропонують персональні послуги.
Over the last few years, the mobile and wireless market has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to the GSM Association and Ovum, the number of mobile subscribers exceeded 2 billion in September 2005, and now exceeds 2,5 billion.	За останні кілька років ринок мобільного і безпровідного зв'язку став одним з найбільш швидкозростаючих ринків у світі, і він продовжує зростати швидкими темпами. За даними Асоціації GSM і Ovum, кількість абонентів мобільного зв'язку перевищила 2 млрд. у вересні 2005 року, і на сьогодні перевищує 2,5 млрд. осіб.
According to a study by financial consultancy Celent, 35 % of online banking households will be using mobile banking. Mobile banking will eventually allow users to make payments at the physical point of sale. "Mobile contactless payments" will make up 10 % of the contactless market.	Згідно з дослідженнями фінансових консультантів Celent 35 % родин, що зараз використовують онлайн-банкінг, стануть користувачами мобільного банкінгу. Мобільний банкінг також дозволить користувачам здійснювати платежі у стаціонарному пункті продажу. «Мобільні безконтактні платежі» складуть 10 % безконтактного ринку.
Many believe that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries like India, China, Bangladesh, Indonesia and Philippines, where mobile infrastructure is comparatively better than the fixed-line infrastructure, and in European countries, where mobile phone penetration is very high, mobile banking is likely to appeal even more.	Багато хто вважає, що мобільні користувачі тільки-но почали повною мірою використовувати потенціал даних у своїх мобільних телефонах. В азіатських країнах, таких як Індія, Китай, Бангладеш, Індонезія і Філіппіни, де мобільна інфраструктура краща, ніж інфраструктура провідних ліній, і в європейських країнах, де поширені мобільні телефони, мобільний банкінг, імовірно, може стати ще більш популярним.
This opens up huge markets for financial institutions interested in	Це відкриває величезні ринки для фінансових установ, зацікавлених у

offering value added services. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while travelling, receiving online updates of stock price or even performing stock trading while being stuck in traffic.	наданні послуг з доданою вартістю. За допомогою мобільних технологій банки можуть запропонувати широкий спектр послуг для своїх клієнтів, таких як грошові перекази під час поїздки, отримання оновлень онлайнового курсу акцій, чи, навіть, виконання торгівельних операцій з цінними паперами під час того, як ви застрягли у пробці.
In the past decades, banks across the globe have invested billions of dollars to build sophisticated internet banking capabilities. As the trend is shifting to mobile banking, there is a challenge for CIOs and CTOs of these banks to decide on how to leverage their investment in internet banking and offer mobile banking, in the shortest possible time.	Протягом останніх десятиріч банки по усьому світу інвестували мільярди доларів для розробки високотехнологічних можливостей інтернет-банкінгу. Наявність тенденції переходу до використання мобільного банкінгу ставить певні завдання для IT-директорів і технічних директорів цих банків з вирішення питань залучення інвестицій в інтернет-банкінг і запровадження мобільного банкінгу у найкоротший термін.
The proliferation of the 3G (third generation of wireless) and widespread implementation expected for the beginning of the century will generate the development of more sophisticated services such as multimedia and links to m-commerce services.	Швидке поширення і широке впровадження технології 3G (третє покоління безпровідного зв'язку), очікуване на початку сторіччя, зумовить розвиток більш високотехнологічних послуг, таких як мультимедіа і послуги мобільної комерції.

Module 5. What Are Next Big Innovations For Personal Banking?

Ex 5.1. Pre-reading: answer the questions:

1. What do you think, do we need several more innovations to facilitate our lives
2. What kind of innovations would you provide

Ex 5.2. Read the following text

What Are Next Big Innovations For Personal Banking?

What are the next **disruptions** for personal financial services? Are they ready for a full "reset"? Can they develop new **perspectives** fast enough and overcome their dogmas? How do we inject out-of-the box thinking and make them work within-the-box? Or can we re-shape the box? The last 6 weeks, we've been focusing some of the most interesting paradigm shifting ideas of how to transform banking, insurance and healthcare. Back to personal banking, there are so many opportunities for innovation.

Here's interesting one. **IPhone check deposit**. One of the US military banks recently **launched mobile check-deposit technology**, which lets users **deposit checks** from anywhere using an iPhone. Customers take photos of both sides of a check with the phone and **transmit the images** to the bank, which then verifies and makes the deposit.

The bank has just one branch and, because of its military legacy, has customers in some Asian countries. That is so cool because it integrates with existing checking habits. 17 % of all its customers across investing, insurance and banking use **mobile apps**, which also facilitates on-phone trading, filing claims for auto accidents, loan calculations and the usual access to account information.

The future of banking is mBanking. The phone will become your wallet (contactless payments), your branch (for deposit) and your credit card. Just don't lose

it. We're prototyping a number of cool mobile wallet and developing scenarios how they would fit it into a social-media culture. And what it means for SMEs etc.

Nokia will be a big player and could use P2P payments as an **entry-point** to emerging markets and a new **revenue stream**. It's launched Nokia Money, a service that lets users make financial transactions on their phones. With Nokia Money, which will start **to roll out** in undisclosed markets, mobile users can send money to other mobile users, pay merchants and **utility bills**, or top up prepaid cellphone minutes. I think more will join. We will end up having Nokia Money, iPhone Dollars, Tata Rupees, Ericsson Krona. Then we will need another kind of **currency exchange**.

Ex 5.3. Answer the following questions

1. What are the new innovations in personal banking services?
2. How does the mobile check-deposit technology work?
3. Why do customers use mobile apps?
4. How does Nokia Money technology work?

Ex 5.4. Match the following definitions

a) disruption	1) рахунки за комунальні послуги
b) perspectives	2) з'явитися
c) paradigm	3) точка входу
d) deposit checks	4) потік прибутку
e) mobile apps	5) обмін валют
f) entry-point	6) перспективи
g) revenue stream	7) збій
h) roll out	8) мобільні програми
i) utility bills	9) парадигма
j) currency exchange	10) передавати зображення
k) iPhone check deposit	11) вносити чекові депозити
l) launch mobile check-deposit technology	12) перевірка депозиту через айфон
m) transmit the images	13) запровадити технологію мобільної перевірки депозиту

Ex 5.5. Complete the following sentences from the words from the box

currency exchange, mobile apps, revenue stream, roll out, utility bills, paradigm, insurance, mobile check-deposit technology, phone check deposit

1. The last 6 weeks, we've been focusing some of the most interesting …… shifting ideas of how to transform banking, ……. and healthcare.
2. There are so many opportunities for innovation. The one of them is …… …… ……
3. One of the US military banks recently launched …… …… ……, which lets users deposit checks from anywhere using an iPhone.
4. 17 % of all its customers across investing, insurance and banking use …… ……..

5. Nokia will be a big player and could use P2P payments as an entry-point to emerging markets -and a new …… ……...

6. With Nokia Money, which will start to …… ……. in undisclosed markets, mobile users can send money to other mobile users, pay merchants and …… ……., or top up prepaid cellphone minutes.

7. We will end up having Nokia Money, iPhone Dollars, Tata Rupees, Ericsson Krona. Then we will need another kind of …… ……...

Ex 5.6. Insert the prepositions

for, from, across, to, of, out, up

1. There are so many opportunities…innovation.
2. One of the US military banks recently launched mobile check-deposit technology, which lets users deposit checks ……. anywhere using an iPhone.
3. The bank has just one branch and, because … its military legacy, has customers in some Asian countries.
4. 17 % of all its customers ……. investing, insurance and banking use mobile apps, which also facilitates on-phone trading, filing claims for auto accidents, loan calculations and the usual access … account information.
5. We're prototyping a number … cool mobile wallet and developing scenarios how they would fit it into a social-media culture.
6. With Nokia Money, which will start to roll … in undisclosed markets, mobile users can send money… other mobile users, pay merchants and utility bills, or top up prepaid cellphone minutes.
7. We will end …. having Nokia Money, iPhone Dollars, Tata Rupees, Ericsson Krona.

Ex 5.7. Translate words and word-combinations into Ukrainian

Disruption; perspectives; paradigm; mobile apps; entry-point; revenue stream; to roll out; utility bills; currency exchange; iPhone check deposit; launch mobile check-deposit technology; transmit the images

Ex 5.8. Translate words and word combinations into English

Рахунки за комунальні послуги; з'явитися; точка входу; потік доходу; обмін валют; перспективи; збій; мобільні програми; парадигма; передавати зображення; перевірка депозиту через айфон; запровадити технологію мобільної перевірки депозиту.

Ex 5.9. Translate sentences into Ukrainian

1. iPhone check deposit lets users deposit checks from anywhere using an iPhone.
2. Customers take photos of both sides of a check with the phone and transmit the images to the bank, which then verifies and makes the deposit.

3. Mobile apps, which also facilitate on-phone trading, filing claims for auto accidents, loan calculations and the usual access to account information.

4. The phone will become your wallet (contactless payments), your branch (for deposit) and your credit card

5. It's launched Nokia Money, a service that lets users make financial transactions on their phones. 6. Mobile users can send money to other mobile users, pay merchants and utility bills, or top up prepaid cellphone minutes.7. We will end up having Nokia Money, iPhone Dollars, Tata Rupees, Ericsson Krona. Then we will need another kind of currency exchange.

Ex 5.10. Translate sentences into English

1. Існує безліч можливостей для впровадження інновацій.

2. Один із найцікавіших прикладів – система завантаження чеків через айфон.

3. Клієнти просто фотографують обидві сторони чека, а потім передають зображення в банк, який його перевіряє та сплачує.

4. 17 % клієнтів, що користуються послугами інвестування, страхування та банкінгу, використовують мобільні програми, які полегшують телефонну комерцію, заповнення позовів стосовно ДТП, розрахунок кредитів та звичайний доступ до інформації по рахунку.

5. Користувачі мобільних телефонів можуть висилати гроші іншим користувачам, сплачувати рахунки та комунальні послуги або заздалегідь поповнити телефонний рахунок.

Ex 5.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

What are the next disruptions for personal financial services? Can they develop new perspectives fast enough and overcome their dogmas? How do we inject out-of-the box thinking and make them work within-the-box? The last 6 weeks, we've been focusing some of the most interesting paradigm shifting ideas of how to transform banking, insurance and healthcare. Back to personal banking, there are so many opportunities for innovation.	Яких наступних збоїв у сфері персональних фінансових послуг треба очікувати? Чи зможуть вони розробити нові напрямки достатньо швидко та подолати свої догми? Як ми інкорпоруємо традиційну технологію у високотехнологічну? Останні шість тижнів ми сконцентрували свою увагу на найбільш цікавій парадигмі ідей, що змінює систему послуг банкінгу, страхування та медичного обслуговування. Стосовно персонального банкінгу, існує безліч можливостей для впровадження інновацій.

Here's interesting one. iPhone check deposit. Customers take photos of both sides of a check with the phone and transmit the images to the bank, which then verifies and makes the deposit.	Один із найцікавіших прикладів – система завантаження чеків через айфон. Клієнти просто фотографують обидві сторони чека, а потім передають зображення в банк, який їх перевіряє, а потім оплачує.
17 % of all its customers across investing, insurance and banking use mobile apps, which also facilitates on-phone trading, filing claims for auto accidents, loan calculations and the usual access to account information.	17 % клієнтів, що користуються послугами інвестування, страхування, та банкінгу, використовують мобільні програми, які також полегшують оплату телефону, заповнення позовів стосовно ДТП, розрахунок кредитів та звичайний доступ до інформації рахунку.
The future of banking is mBanking. We're prototyping a number of cool mobile wallet and developing scenarios how they would fit it into a social-media culture.	Майбутнє банкінгу – це мобільний М-банкінг. Ми працюємо над серією прототипів сучасних мобільних гаманців, а також розробляємо план дій, як запровадити їх використання у соціальній культурі засобів масової інформації.
Nokia will be a big player and could use P2P payments as an entry-point to emerging markets and a new revenue stream. With Nokia Money, which will start to roll out , mobile users can send money to other mobile users, pay merchants and utility bills, or top up prepaid cellphone minutes.	Компанія Nokia буде відігравати важливу роль і зможе використовувати засоби сплати (з'єднання рівноправних вузлів) як відправної точки до новоствореного ринку і нового потоку доходів. За допомогою електронних грошей Nokia, які почнуть незабаром з'являтися, користувачі мобільних телефонів можуть висилати гроші іншим користувачам мобільного зв'язку, сплачувати рахунки та комунальні послуги або заздалегідь поповнити телефонній рахунок.

Module 6. Missed Opportunity

Ex 6.1. Pre-reading: answer the questions:

1. Do you know any convenient ways to pay bills? If you do, name them.
2. What are the advantages to pay bills the way you've just named?

Ex 6.2. Read the text

Missed Opportunity

Are banks missing opportunities to offer more useful bill-payment services?

The threat of **disintermediation** is wide and varied in financial services. Financial institutions have benefited greatly from bill pay; it's an integral reason why more consumers didn't switch during last Bank Transfer Day.

Banks have reported in the past that when customers sign up for online bill payment, customer retention skyrockets. In Javelin's survey of 4,728 consumers conducted last December, 83 % of those who paid all their bills through their financial institution were satisfied with their current banking relationship. Among those who paid their bills through their billers' websites, 73 % said they were satisfied with their current financial institution.

A financial institution that's blinding itself to the threat that other companies can't steal a piece of their business is vulnerable. If somebody else can convince the consumer that he would get a better way to pay bills, that's a significant threat to a financial institution.

For instance, nonbank bill-payment providers could let consumers pay all their bills in one place, for all bank accounts and all billers, providing a big-picture view of the consumer's finances.

The nonbanks could also potentially provide more **flexibility**. While a financial institution will typically let people pay bills with their checking account, an outside provider could let people use a credit card or other payment method.

We have reams of evidence that consumers have complex financial lives, frequently are dealing with a lot of products and financial institutions, and have bills all over the place. The more they move to a **digital lifestyle**, the more they'll say they need help to tame the mess and bring order to it. What they really want is some way to **consolidate the chore**, make it easier, all in one place with control.

What many banks have today is an "**entanglement strategy**" in which they're good at **keeping customers in bill-payment relationships** simply because it's very hard to **unwind these accounts**. One could take the view that the thing that's great about bill pay is it entangles consumers and they'll be too tied up in a spider web to get away.

Banks would be better off focusing on finding a way to make their bill-payment services so good that consumers wouldn't even consider trying to unravel them.

A weakness of the nonbank innovators is their lack of mobile offerings. Banks have been offering mobile alerts to let people know about bill payments, potential fraud and potential **overdrafts** for several years, though not always perfectly.

Getting alerts right could give the consumer the sense that he's got always-on control and access to his money, and help the bank provide a personal relationship through electronic means.

The personal part is it's about your account, what just happened, what you need to do. That's going to be another reason why financial institutions are in a better spot to build on their bill-payment relationships and not let them **erode**.

Bill-payment innovators will probably build their products in four phases: they will work on money management, then tie bill payment to financial management, then offer mobile access to these services and, finally, offer archival of bills.

They will have to be patient, because consumers aren't **clamoring** for an archiving solution right now. They've got reams of digital stuff, but they're going to have to see proof that it can be done in a way that's simple and safe.

Ex 6.3. Answer the questions:

1. What can happen with the customer retention when he signs up for online bill payment?
2. What services can nonbank bill-payment providers offer?
3. What is the main weakness of the nonbank innovators?
4. What are the advantages of bank’s institutions?

Ex 6.4. Match the Ukrainian translations to the English phrases:

a) disintermediation	1) концентрація, важка (рутинна) робота
b) flexibility	2) перевищення кредиту
c) consolidate chore	3) вилучення грошей з банківських рахунків
d) entanglement strategy	4) стратегія утримання клієнтів
e) overdrafts	5) наполягати на
f) clamour for	6) гнучкість
g) digital lifestyle	7) спосіб життя, що потребує цифрових

h) keep customers in bill-payment relationships i) unwind the account j) erode	технологій 8) руйнувати 9) закривати рахунок 10) утримати клієнтів завдяки їх потребам оплати рахунків

Ex 6.5. Complete the following sentences from the words from the box.

disintermediation, unwind, flexibility, "entanglement strategy", skyrockets, clamor, overdraft, erode

1. The threat of ……. is wide and varied in financial services.
2. Banks have reported in the past that when customers sign up for online bill payment, customer retention ……...
3. The nonbanks could also potentially provide more……...
4. What many banks have today, is an "…… ……." in which they're good at keeping customers in bill-payment relationships simply because it's very hard to ……these accounts.
5. Banks have been offering mobile alerts to let people know about bill payments, potential fraud and potential ……. for several years, though not always perfectly.
6. That's going to be another reason why financial institutions are in a better spot to build on their bill-payment relationships and not let them ……
7. They will have to be patient, because consumers aren't …….. for an archiving solution right now.

Ex 6.6. Insert the prepositions.

from, at, on, up, to, off

1. Financial institutions have benefited greatly …. bill pay; it's an integral reason why more consumers didn't switch during last Bank Transfer Day.
2. Banks have reported in the past that when customers sign … for online bill payment, customer retention skyrockets.
3. What many banks have today is an "entanglement strategy" in which they're good ... keeping customers in bill-payment relationships simply because it's very hard to unwind these accounts.
4. Bill-payment innovators will probably build their products in four phases: they will work … money management, then tie bill payment to financial management, then offer mobile access … these services and, finally, offer archival of bills.
5. Banks would be better … focusing on finding a way to make their bill-payment services so good that consumers wouldn't even consider trying to unravel them.

Ex 6.7. Here are the answers. Work out the questions.

1. The threat of disintermediation is wide and varied in financial services.

2. A financial institution that's blinding itself to the threat that other companies can't steal a piece of their business is vulnerable. If somebody else can convince the consumer that he would get a better way to pay bills, that's a significant threat to a financial institution.

3. Banks have been offering mobile alerts to let people know about bill payments, potential fraud and potential overdrafts for several years, though not always perfectly.

4. The personal part is it's about your account, what just happened, what you need to do. That's going to be another reason why financial institutions are in a better spot to build on their bill-payment relationships and not let them erode.

5. Bill-payment innovators will probably build their products in four phases: they will work on money management, then tie bill payment to financial management, then offer mobile access to these services and, finally, offer archival of bills.

Ex 6.8. Give the English equivalent.

Об'єднатися; важка робота; перевищення кредиту; вилучення грошей з банківських рахунків; стратегія утримання клієнтів; обурюватися; гнучкість; цифровий спосіб життя; руйнувати; закривати рахунок; утримати клієнтів завдяки їх потребам оплати рахунків.

Ex 6.9. Give the Ukrainian equivalent

Disintermediation; flexibility; consolidate; chore; entanglement strategy; overdraft; to clamour; digital lifestyle; keep customers in bill-payment relationships; unwind the account; erode.

Ex 6.10. Translate sentences into English

1. Посередництво дуже поширене серед фінансових послуг.
2. Фінансові інститути отримують значний прибуток від оплати рахунків.
3. На сьогодні банки ведуть стратегію утримання клієнтів завдяки їх потребам оплати рахунків.
4. Фінансові установи вводять себе в оману, закриваючи очі на загрозу, що інші компанії можуть вкрасти частину їх бізнесу.
5. Найбільша слабкість кредитно-фінансових установ полягає у відсутності різноманітних мобільних пропозицій. Банки завжди попереджають клієнтів стосовно оплати рахунків, потенційної крадіжки або потенційного перевищення кредиту.
6. Сконцентрувати в одному місці рутинну роботу, зробити її легшою – ось чого насправді хочуть клієнти.
7. Кредитно-фінансові установи могли б дозволити клієнтам оплачувати усі їх рахунки в одному місці, при цьому надаючи повну інформацію про стан фінансів клієнта.

Ex 6.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Are banks missing opportunities to offer more useful bill-payment services?	Чи можуть банки втратити можливість запропонувати клієнтам більш зручні послуги оплати рахунків?
The threat of disintermediation is wide and varied in financial services. Financial institutions have benefited greatly from bill payment.	Існує загроза втрати посередництва, яке є дуже поширеним та різноманітним серед фінансових послуг. Фінансові інститути отримують значний прибуток від оплати рахунків.
Banks have reported in the past that when customers sign up for online bill payment, customer retention skyrockets.	Банки повідомили, що як тільки клієнти погоджуються на послуги оплати рахунків онлайн – різко підвищується їх спроможність утримання клієнтів.
A financial institution that's blinding itself to the threat that other companies can't steal a piece of their business is vulnerable. If somebody else can convince the consumer that he would get a better way to pay bills, that's a significant threat to a financial institution.	Фінансові установи, які вводять себе в оману, закриваючи очі на загрозу, що інші компанії не можуть вкрасти частину їх бізнесу, є вразливими. Якщо хтось зможе запевнити клієнта, що існує зручніший спосіб оплати рахунків, то це може стати значною загрозою для фінансової установи.
For instance, nonbank bill-payment providers could let consumers pay all their bills in one place, for all bank accounts and all billers, providing a big-picture view of the consumer's finances.	Наприклад кредитно-фінансові установи могли б дозволити клієнтам оплачувати усі їх рахунки в одному місці для всіх банківських рахунків та платників, при цьому надаючи повну інформацію про фінанси клієнта.
The nonbanks could also potentially provide more flexibility. While a financial institution will typically let people pay bills with their checking account, an outside provider could let people use a credit card or other payment method.	Кредитно-фінансові установи потенційно могли б бути більш гнучкими. В той час як фінансові установи зазвичай будуть дозволяти клієнтам оплачувати послуги тільки з їх поточних чекових рахунків, інші установи могли б дозволити використовувати кредитні картки або інші способи оплати.

What consumers really want is some way to consolidate the chore, make it easier, all in one place with control.	Сконцентрувати рутинну роботу в одному місці, зробити її легшою і підконтрольною – ось що насправді хочуть клієнти.
Bill-payment innovators will probably build their products in four phases: they will work on money management, then tie bill payment to financial management, then offer mobile access to these services and, finally, offer archival of bills.	Інноватори засобів оплати рахунків, імовірно, створять процедуру проходження чотирьох станів: вони працюватимуть над системою управління грошами, потім об'єднають оплату рахунків з управлінням фінансами, а потім запропонують мобільний доступ до всіх послуг, і нарешті, запропонують архівацію рахунків.
They will have to be patient, because consumers aren't clamoring for an archiving solution right now. They've got reams of digital stuff, but they're going to have to see proof that it can be done in a way that's simple and safe.	Вони мають бути терплячими, адже клієнти не потребують вирішення питання стосовно архіву саме зараз. У клієнтів є безліч цифрових приладів, але вони бажають отримати доказ, що це можна робити простішим та безпечнішим способом.

Module 7. Internet Banking Integration within the Banking System

Ex 7.1. Pre-reading: answer the questions:

1. How do you understand the notion «internet banking integration»?
2. What in your opinion are the advantages of internet banking integration?

Ex 7.2. Read the text below:

Internet Banking Integration within the Banking System

Internet has changed very much the rules of the game in the past years. The banking area of the economic sector was **impacted** by those changes as well. Customers' requests for quick access and no matter the location at their bank accounts, or at financial/banking transactions, all of these have determined the banking institutions worldwide **to adopt** the Internet as the optimal solution for the presented demands. Through the Internet network banks are able to connect **front-end (front-office) applications** with **back-end (back-office).** Based on such advantages, Internet Banking applications were created.

The evolution of bank presence on Web from simple, static applications, to complex, dynamic applications with numerous transactions, is presented bellow: Until 2000, Internet Banking applications could have been accessed mostly in the United States of America, or in European countries such as: United Kingdom, Spain, Italy and France. Since 2000, online banking applications are **commercialized** or created in other countries.

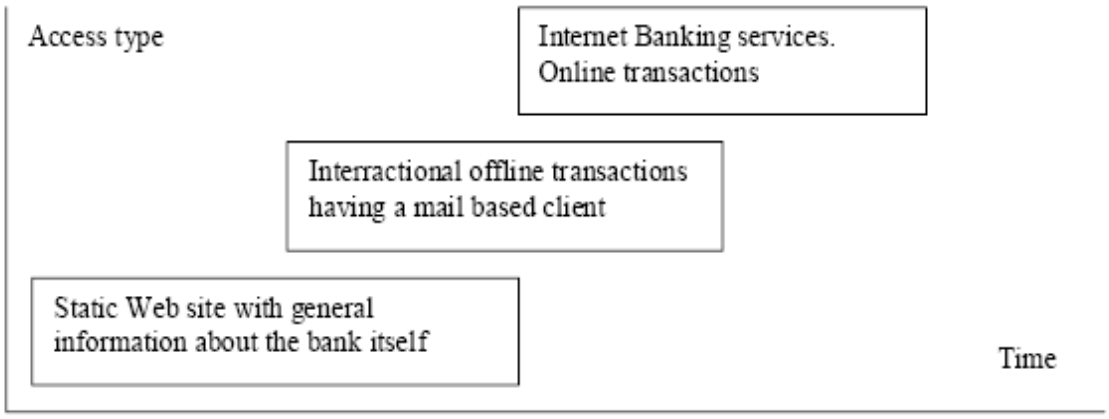


Fig.1. Bank evolution on Web

The advantages of Internet Banking applications consist of: quickness; **secured access to** sensitive data as accounts, personal data of customers, transactions; account management; operating **sale-purchase transactions** in real time and at long distance**; suppressing** the stress of staying in bank for a transaction; low costs for the maintenance of this kind of applications. Internet determined also the appearance of first **service-oriented architectures (SOA)**. This architecture can be used to interact on Internet or from a **workstation** to another (using point-to-point protocols for data transfer – EDI, electronic data interchange). SOA is basically built from software services. These services are independent one from each other and they run protected on the working platforms (application servers): .NET or Java. These have the ability to manage the memory, to create the synchronous or asynchronous links between different components and to create the **data mapping**. The architecture is presenting itself as a summary of services: SOA architectures helped banks by offering them the possibility to connect different applications or to integrate big portions of software code in **ad hoc applications**. This is one of the reasons why SOA became a key element in Internet Banking applications.

Internet Banking represents an interface of banking operations directly with the customers, which is integrated with the back-end system of the bank.

By the Internet and Intranet development, the banking market faced a healthy growth. Customer's demands influenced the **ascension.**

Internet banking application is like a black-box. Ideally, the communication with the back-end will be asynchronous. The reason for this type of communication is that the system will be able to run as a whole 24 hours out of 24. The Web application will run continuously, even if the back-end becomes unavailable. Of course, this is **bidirectional,** meaning when the Web is not available, the back-end will continue working (specific processes of the back-end application will run no matter the front-end is active or not). Also, the back-end sees the front-end as a number of services with big **granularities.** In this way a bigger generality is **assured** for the integration solution. This is the standard that SOA proposes to different businesses.

Along with the development of the Internet, banks needed to **adapt** their informatics systems in order to answer to customers' demands in an efficient manner.

Therefore, there were several services oriented architectures implemented, that could integrate existing back-end applications completed by front-end applications, new from the building technology point of view.

A key element of front office applications is Internet Banking, because it allows **remote access,** it is secured, flexible, permits online transactions, in real time, as if operations were teller ones, without suffering from stress of queues.

Due to high costs of complex informatics systems, big companies and banks have started using SOA architectures (service-oriented architecture). SOA offers banks the possibility of connecting older applications to new ones, including the integration of Internet Banking in the current customized system. SOA can be used for a wide range of operating systems, **application servers** and **data bases,** according to budget and performance limitations of the **beneficiary**.

Ex 7.3. Answer the questions:

1. What for were the internet banking applications created for?
2. What are the main advantages of the internet banking applications?
3. How do the banks decide the service-oriented problems?
4. What abilities does the SOA possess?
5. Why has the SOA become a key element for the internet banking applications?

Ex 7.4. Match the Ukrainian translations to the English phrases:

a) impact	1) впливати
b) adopt	2) база даних
c) front-end (front-office) application	3) приймати
	4) отримувач прибутку
d) commercialize	5) первинні (інтерфейсні) прикладні програми
e) secured access to	6) віддалений доступ
f) sale-purchase transaction	7) пристосовуватися
g) suppress	8) перетворювати в джерело прибутку (видобувати прибуток)
h) service-oriented architectures (SOA)	9) гарантований доступ до
i) data mapping	10) гарантувати
j) ad hoc application	11) ступінь деталізації
k) ascension	12) транзакції купівлі-продажу
l) bidirectional	13) двонаправлений
m) granularities	14) підйом
n) assure	15) стримувати
o) adapt	16) спеціальна прикладна програма
p) remote access	17) відображення даних
q) beneficiary	18) схема для обслуговування широкого кола запитів
r) data base	
s) back-end (back-office)	19) фоновий додаток

Ex 7.5. Complete the following sentences from the words in the box

beneficiary, data bases, application servers, ascension, remote access, service-oriented architectures (SOA), impact, front-end (front-office) applications, back-end (back-office), secured access to, sale-purchase transactions, workstation, suppressing

1. Internet has changed very much the rules of the game in the past years. The banking area of the economic sector was ……... by those changes as well.

2. Through the Internet network banks are able to connect …… …… …… with …… ……...

3. The advantages of Internet Banking applications consist of: quickness; …… …… sensitive data as accounts, personal data of customers, transactions; account management; operating …… …… …….. in real time and at long distance; …….. the stress of staying in bank for a transaction; low costs for the maintenance of this kind of applications.

4. …… …… ……- can be used to interact on Internet or from an ……. to another (using point-to-point protocols for data transfer – EDI, electronic data interchange).

5. By the Internet and Internet development, the banking market faced a healthy growth. Customer's demands influenced the……...

6. Internet Banking allows …… …….. It is secured, flexible, permits online transactions, in real time, as if operations were teller ones, without suffering from stress of queues.

7. SOA can be used for a wide range of operating systems, …… …….. and …… …….. according to budget and performance limitations of the …….

Ex 7.6. Insert the prepositions

by, with, of, for, at, on

1. The banking area of the economic sector was **impacted** … those changes as well.

2. Customers requests … quick access and no matter the location … their bank accounts, or at financial/banking transactions, all of these have determined the banking institutions world wide **to adopt** the Internet as the optimal solution … the presented demands.

3. Based … such advantages, Internet Banking applications were created.

4. The advantages …Internet Banking applications consist …: quickness; **secured access to** sensitive data as accounts, personal data of customers, transactions; account management; operating **sale-purchase transactions** in real time and at long distance; **suppressing** the stress of staying in bank for a transaction; low costs … the maintenance of this kind of applications.

5. Internet Banking represents an interface of banking operations directly with the customers, which is integrated ….. the back-end system of the bank.

Ex 7.7. Here are the answers. Work out the questions:

1. Until 2000, Internet Banking applications could have been accessed mostly in the United States of America, or in European countries such as: United Kingdom, Spain, Italy and France.

2. The advantages of Internet Banking applications consist of: quickness; **secured access to** sensitive data as accounts, personal data of customers, transactions; account management; operating **sale-purchase transactions** in real time and at long distance; **suppressing** the stress of staying in bank for a transaction; low costs for the maintenance of this kind of applications.

3. **SOA** architecture can be used to interact on Internet or from a **workstation** to another (using point-to-point protocols for data transfer – EDI, electronic data interchange).

4. SOA architectures helped banks by offering them the possibility to connect different applications or to integrate big portions of software code in **ad hoc applications**.

5. Internet Banking represents an interface of banking operations directly with the customers, which is integrated with the back-end system of the bank.

Ex 7.8. Translate into Ukrainian

To be impacted by changes; to adopt; front-end (front-office) applications; back-end (back-office); online banking applications are commercialized; secured access to sensitive data; sale-purchase transactions; workstation; service-oriented architectures (SOA); data mapping; ad hoc applications; ascension; to adapt; to be assured for; key element; application servers; data bases.

Ex 7.9. Translate into English

Зазнати впливу; база даних; приймати; бенефіціар; первинні (інтерфейсні) прикладні програми; віддалений доступ; пристосовуватися; перетворювати в джерело добутку (видобувати прибуток); гарантований доступ до; гарантувати; ступень деталізації; транзакції купівлі-продажу; двонаправлений; підйом; стримувати; спеціальна прикладна програма; відображення даних; схема для обслуговування широкого кола запитів.

Ex.7.10. Translate sentences into Ukrainian:

1. Internet has changed very much the rules of the game in the past years, and the banking area of the economic sector was impacted by those changes as well.

2. Through the Internet network banks are able to connect **front-end (front-office) applications with back-end (back-office)**.

3. Until 2000, Internet Banking applications could have been accessed mostly in the United States of America, or in European countries such as: United Kingdom, Spain, Italy and France, and since 2000, online banking applications are **commercialized** or created in other countries.

4. The advantages of Internet Banking applications consist of: quickness; **secured access to** sensitive data as accounts, personal data of customers, transactions; account management; operating **sale-purchase transactions** in real time and at long distance; suppressing the stress of staying in bank for a transaction; low costs for the maintenance of this kind of applications. Internet determined also the appearance of first's **service-oriented architectures (SOA)**.

5. Internet Banking represents an interface of banking operations directly with the customers, which is integrated with the back-end system of the bank.

6. This architecture can be used to interact on Internet or from an **workstation** to another.

7. A key element of front office applications is Internet Banking, because it allows **remote access**, it is secured, flexible, permits online transactions, in real time, as if operations were teller ones, without suffering from stress of queues.

Ex 7.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

The banking area of the economic sector was impacted by changes. Customers requests for quick access and no matter the location at their bank accounts, or at financial/banking transactions, all of these have determined the banking institutions world wide to adopt the Internet as the optimal solution for the presented demands. Through the Internet network banks are able to connect front-end (front-office) applications with back-end (back-office).	В економічному секторі банківська діяльність зазнала змін. Клієнти вимагають швидкого доступу незважаючи на місця розташування їх банківських рахунків або фінансових/банківських транзакцій, тому всі банківські установи по всьому світу визнали інтернет як оптимальне рішення для представлених вимог. Завдяки Інтернету банки можуть з'єднувати первинні (інтерфейсні) прикладні програми з фоновими програмами.
The advantages of Internet Banking applications consist of: quickness; secured access to sensitive data as accounts, personal data of customers, transactions; account management; operating sale-purchase transactions in real time and at long distance; suppressing the stress of staying in bank for a transaction; low costs for the maintenance of this kind of applications. Internet determined also the appearance of firsts service-	Переваги прикладного програмного забезпечення інтернет-банкінгу складаються з: швидкості; гарантованого доступу до чутливих даних, таких як рахунки, особисті дані клієнтів, транзакції; управління рахунками; керування платіжньо-купівельними транзакціями на великій відстані; звільнення від тиску банку для транзакції; низькі витрати для обслуговування цього виду програм. За допомогою інтернету з'явилася схема для

oriented architectures (SOA). This architecture can be used to interact on Internet or from an workstation to another. SOA is basically built from software services. The architecture is presenting itself as a summary of services: SOA architectures helped banks by offering them the possibility to connect different applications or to integrate big portions of software code in ad hoc applications. This is one of the reasons why SOA became a key element in Internet Banking applications. Internet banking application is like a black-box. The Web application will run continuously, even if the back-end becomes unavailable. Of course, this is bidirectional, meaning when the Web is not available, the back-end will continue working. Due to high costs of complex informatics systems, big companies and banks have started using SOA architectures (service-oriented architecture). SOA offers banks the possibility of connecting older applications to new ones, including the integration of Internet Banking in the current customized system. SOA can be used for a wide range of operating systems, application servers and data bases, according to budget and performance limitations of the beneficiary.	обслуговування широкого кола запитів (SOA). Ця схема дає можливість взаємодії в інтернеті або між різними автоматизованими робочими місцями. SOA в основному базується на програмному забезпеченні. Схема являє собою сукупність послуг: архітектура SOA надала банкам можливість з'єднати різні прикладні програми або об'єднати великі частини коду програмного забезпечення в спеціалізованих прикладних програмах. Це одна з причин, чому SOA стала ключовим елементом у прикладному програмному забезпеченні інтернет-банкінг. Прикладне програмне забезпечення інтернет-банкінг подібне до чорного ящика. Прикладна програма працюватиме безперервно, навіть якщо банківський відділ із транзакцій стане недоступним. Зазвичай ця система двонаправлена, тобто, коли мережа недоступна, банківський відділ з транзакцій продовжуватиме працювати. Через високу ціну складних інформаційних систем великі компанії і банки почали використовувати систему SOA. SOA пропонує банкам можливість з’єднання старих прикладних програм з новими, у тому числі інтеграцію нтернет-банкінгу у модифіковану згідно із запитами клієнта систему. SOA може використовуватися для широкого кола операційних систем прикладних серверів і бази даних згідно з обмеженнями бюджету і роботи власника.

Module 8. Internet Banking Risks

Ex 8.1 Pre-reading: answer the questions:

1. What kinds of risks for the bank supervision do you know?
2. Can you think of any credit risks in banks of your banks of your country?

Ex 8.2 Read the following text

Internet Banking Risks

Internet banking creates new risk control challenges for national banks. The **OCC** has defined nine categories of risk for bank **supervision** purposes. The risks are credit, **interest rate**, **liquidity**, price, **foreign exchange**, transaction, **compliance**, strategic, and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

Credit Risk

Credit risk is the risk to earnings or capital arising from an **obligor's** failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk is found in all activities where success depends on **counterparty, issuer**, or **borrower** performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the **bank's balance sheet.** Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the world. In dealing with customers over the Internet, absent any personal contact, it is challenging for institutions to **verify** the **bona fides** of their customers, which is an important element in making **sound credit decisions**. Unless properly managed, Internet banking could lead to a concentration in **out-of-area** credits or credits within a **single industry.**

Interest Rate Risk

Interest rate risk is the risk to earnings or capital arising from **movements** in interest rates. **From an economic perspective**, a bank focuses on the sensitivity of the value of its **assets**, **liabilities** and **revenues** to changes in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing of **cash flows** (**repricing risk);** from changing rate relationships among different **yield**

curves affecting bank activities **(basis risk**); from changing rate relationships across the **spectrum** of **maturities (yield curve risk**); and from **interest-related options embedded** in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid **hedging** strategies or products. Internet banking can attract deposits, **loans,** and other relationships from a larger pool of possible customers than other forms of marketing.

Liquidity Risk

Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without **incurring** unacceptable **losses.** Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions affecting the ability of the bank **to liquidate** assets quickly and with minimal loss in value.

Foreign Exchange Risk

Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency. Foreign exchange risk can be intensified by political, social, or economic developments. The consequences can be unfavorable if one of the currencies involved becomes subject to stringent exchange controls or is subject to wide **exchange-rate fluctuations.**

Transaction Risk

Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Transaction risk is evident in each product and service offered and **encompasses** product development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment. A high level of transaction risk may exist with Internet banking products, particularly if those **lines of business** are not adequately planned, implemented, and monitored.

Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or **nonconformance with,** laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, payment of damages, and the **voiding of contracts**. Compliance risk can lead to a **diminished reputation,** reduced **franchise value,** limited business opportunities, reduced **expansion potential**, and lack of contract enforceability**.**

Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from **adverse business decisions,** improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the **compatibility** of an organization's strategic goals, the business strategies developed to achieve those goals, the resources **deployed against** these goals, and the quality of implementation. The resources needed to carry out business strategies are both **tangible and intangible.** They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to **litigation,** financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community. A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to **customer inquiries**, or violations of customer privacy expectations.

Ex 8.3. Answer the following questions:

1. What are the nine categories of risks for the bank supervision?
2. When does the credit risk arise from?
3. What are the advantages of internet banking?
4. What can result interest rate risk?
5. What factors should be considered during the evaluation of the interest rate risk?
6. What factors can intensify foreign exchange risk?
7. What can cause the compliance risk?

Ex 8.4. Match the Ukrainian translations to the English phrases:

a) bank's balance sheet	1) активи
b) counterparty	2) боржник, дебітор
c) issuer	3) відсоткова ставка
d) obligor	4) правильне рішення
e) supervision	5) впроваджувати
f) interest rate	6) емітент
g) liquidity	7) з економічної точки зору

h) foreign exchange	8) зобов'язання
i) borrower	9) іноземна валюта
j) credit risk	10) конкретна галузь промисловості
k) liabilities	11) контрагент (протилежна сторона)
l) revenue	12) кредити іноземним особам
m) assets	13) ліквідність
n) cash flows	14) нагляд, контроль
o) single industry	15) перевірити чесні наміри
p) sound decisions	16) позика
q) verify the bona fides	17) позичальник
r) out-of-area credits	18) прибуток
s) interest rate risk	19) ризик внаслідок зміни відсоткової ставки
t) from an economic perspective	20) ризик ліквідності
u) loans	21) ризик, пов'язаний з несплатою кредиту
v) liquidity risk	22) рух грошових коштів
w) embed	23) сальдо банківського рахунку
x) hedging	24) хеджування

Ex 8.5. Complete the following sentences from the words from the box:

Supervision, liabilities, out-of-area credits, contract enforceability, diminished reputation, counterparty ,interest rate, borrower, liquidity, foreign exchange, franchise value, voiding of contracts, loans, revenues, assets, single industry, compliance, From an economic perspective, encompass, issuer, expansion potential ,adverse business decisions

1. The committee has defined nine categories of risk for bank **……..** purposes. The risks are credit, **…… ……**, price, **……..**, transaction, **……..**, strategic, and reputation.

2. Credit risk is found in all activities where success depends on **…… ……**, or **…….** performance.

3. Internet banking could lead to a concentration in **……** or credits within a **……...**

4. **……...**, a bank focuses on the sensitivity of the value of it……., **……** and **……** to changes in interest rates.

5. Internet banking can attract deposits,……**,** and other relationships from a larger pool of possible customers than other forms of marketing.

6. Transaction risk is evident in each product and service offered and **……..** product development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

7. Strategic risk is the current and prospective impact on earnings or capital arising from **…… …… ……,** improper implementation of decisions, or lack of responsiveness to industry changes.

8. Compliance risk exposes the institution to fines, payment of damages, and the **…… ……..**

9. Compliance risk can lead to a **…… ……..,** reduced **…… ……,** limited business opportunities, reduced **…… ……..,** and lack of **…… ……..**

Ex 8.6. Insert the preposition

for, on, from, through, with, out

1. Internet banking creates new risk control challenges ….. national banks.
2. Credit risk is found in all activities where success depends …. counterparty, issuer, or borrower performance.
3. It arises any time bank funds are extended, committed, invested, or otherwise exposed …….. actual or implied contractual agreements, whether on or off the banks balance sheet.
4. …… an economic perspective, a bank focuses …. the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates.
5. Compliance risk is the risk to earnings or capital arising ……. violations of, or nonconformance ……. laws, rules, regulations, prescribed practices, or ethical standards.
6. The resources needed to carry …. business strategies are both tangible and intangible.

Ex 8.7. Match the Ukrainian translations to the English phrases:

a) yield curve risk	1) валютний ризик
b) interest-related options	2) франшиза
c) spectrum of maturities	3) діапазон строку платежу
d) basis risk	4) зазнати збитків
e) repricing risk	5) запити клієнтів
f) movement in interests rate	6) зміни у відсоткових ставках
g) customer inquiries	7) коливання обмінних ставок
h) tangible and intangible	8) ліквідувати
i) litigation	9) матеріальні / нематеріальні
j) compatibility	10) несприятливе ділове рішення
k) deploy against	11) опції вибору відсотка
l) expansion potential	12) охоплювати
m) adverse business decisions	13) потенціал розширення
n) diminished reputation	14) принижена репутація
o) franchise	15) ризик недотримання правил
p) voiding of contracts	16) ризик у діапазоні кривої прибутковості
q) lines of business	
r) compliance risk (nonconformance with)	17) ризик, що загрожує діяльності банку
s) foreign exchange risk	18) розгорнути (проти)

t) exchange-rate fluctuations u) encompass v) incur losses w) to liquidate	19) скасування контракту 20) судовий процес 21) сумісність 22) сфера діяльності 23) ціновий ризик

Ex 8.8. Here are the answers. Work out the questions.

1. The committee has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation.

2. Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed.

3. Transaction risk is evident in each product and service offered and encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

4. Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.

5. A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy expectations.

Ex 8.9. Match the term with its definition

a) interest rate b) liquidity c) assets d) issuer e) loans f) cash flows g) compliance risk	1) is a judicial body which is entitled to issue emissive equity 2) is a form of exchange for the global decentralized trading of international currencies 3) is the rate at which interest is paid by a borrower for the use of money that they borrow from a lender 4) is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards 5) is the movement of money into or out of a business, project, or financial product 6) represent ownership of value that can be converted into cash 7) is an asset's ability to be sold without causing a significant movement in the price and with minimum loss of value

Ex 8.10. Translate into Ukrainian

Interest rate; supervision; liquidity; foreign exchange; credit risk; obligor; counterparty; issuer; borrower; bank's balance sheet; verify the bona fides; sound decisions; out-of-area credits; single industry; interest rate risk movement from an economic perspective assets; liabilities; revenue; cash flows; repricing risk; basis risk; spectrum of maturities; yield curve risk; interest-related options; hedging; loans; incur losses; to liquidate; exchange-rate fluctuations; encompass.

Ex 8.11. Translate into English

Коливання обмінних ставок; охоплювати, виконувати; галузь діяльності; ризик згоди; невідповідність до чогось; скасування контракту; принижена репутація; право голосу, франшиза; потенціал розширення; стратегічний ризик; несприятливе ділове рішення; сумісність; розгорнути (проти); матеріальні, нематеріальні; судовий процес; запити клієнтів; відсоткова ставка; нагляд, контроль; ліквідність; валютний ризик; ризик, пов'язаний з несплатою кредиту; боржник, дебітор; контрагент; емітент; позичальник; сальдо банківського рахунку; перевірити чесні наміри; правильне рішення; надання кредитів іноземним особам.

Ex 8.12. Translate sentences into Ukrainian

1. The OCC has defined nine categories of risk for bank supervision purposes. These categories are not mutually exclusive and all of these risks are associated with Internet banking.
2. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance.
3. Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products. Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing.
4. Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses.
5. Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency.
6. Compliance risk exposes the institution to fines, payment of damages, and the voiding of contracts.
7. Strategic risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.

Ex 8.13. Translate the sentences into English

1. Ризик неплатежу за кредитом існує при всіх видах дій, де успіх залежить від контрагента, емітента або роботи позичальника.

2. У роботі з клієнтами через інтернет відсутній будь-який особистий контакт, який може допомогти перевірити чесні наміри клієнтів,що є важливим елементом у прийнятті правильного рішення з приводу видачі кредиту.

3. Надання банківських послуг через інтернет, яке не керується належним чином, може призвести до накопичення кредитів з боржниками з інших країн, або кредитів в межах одного виробництва.

4. Відсотковий ризик – ризик від виручок або капіталу, викликаний коливаннями відсоткових ставок.

5. Відсотковий ризик є результатом відмінностей між вибором часу змін ставок і вибором часу рухів грошових коштів (ціновий ризик); від заміни відношення ставок серед різних кривих прибутковості, що впливають на банківські дії (базовий ризик); від заміни відношення ставок залежно від строків платежу (ризик кривої прибутковості); від вибору, вкладеного в банківську продукцію (ризик вибору).

6. Ризик ліквідності – ризик від виручок або підйому капіталу на нездатності банку відповідати за своїми зобов'язаннями таким чином, щоб не зазнати неприпустимих збитків.

7. Валютний ризик – це ризик, коли позика або портфель позик виражається в іноземній валюті або вкладається в засоби запозичення в іншій валюті.

8. Ризик транзакції – поточний і майбутній ризик від виручок або підйому капіталу на випадок фальсифікації, помилки, нездатності поставляти продукцію або послуги, підтримувати конкурентоспроможну позицію та управляти інформацією.

9. Ризик згоди виникає в ситуаціях, де закони або правила, що управляють певною банківською продукцією або діями клієнтів, можливо, неоднозначні або невипробувані.

Ex 8.14. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

The committee has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation.	Комітет визначив дев'ять категорій ризиків для цільового банківського нагляду. Цими ризиками є: кредит, відсоткова ставка, ліквідність, ціна, валюта, торгові операції, дотримування правил, стратегія і репутація.
Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed. It	Кредитний ризик – це ризик отримання доходів або капіталу, який з'являється, якщо боржник не вкладається в строк оплати, який був вказаний у контракті з банком, чи якось

arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the bank's balance sheet.	інакше порушує домовленості. Ризик виникає у будь-якому випадку, коли банк надає кошти, бере зобов'язання щодо їх виконання, робить інвестиції або іншим чином ризикує коштами відповідно до умов реальних чи умовних угод залежно від сальдо банківського рахунку.
Interest rate risk is the risk to earnings or capital arising from movements in interest rates. Interest rate risk arises: • from differences between the timing of rate changes and the timing of cash flows (repricing risk); • from changing rate relationships among different yield curves affecting bank activities (basis risk); • from changing rate relationships across the spectrum of maturities (yield curve risk); • and from interest-related options embedded in bank products (options risk).	Ризик зміни відсоткової ставки – це наявний або потенційний ризик для надходжень або капіталу, який виникає внаслідок змін відсоткових ставок. Ризик відсоткової ставки є результатом: • відмінностей між термінами ставок і руху грошових потоків (цінових змін); • зміни між ставками у діапазоні кривої прибутковості, що впливає на банківські операції і є загрозою для діяльності банку; • зміни ставок у діапазоні терміну платежу; • вибору відсоткової ставки (ризик вибору опції) банківського продукту.
Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses.	Ризик ліквідності – ризик для надходжень та капіталу внаслідок нездатності банку виконувати свої зобов'язання таким чином, щоб не зазнати неприпустимих збитків.
Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency.	Валютний ризик – це ризик, коли позика або портфель позик виражається в іноземній валюті або в засобах запозичення в іншій валюті.
Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information.	Ризик транзакції – наявний або потенційний ризик для надходжень та капіталу, викликаний фальсифікацією, помилками і нездатністю поставляти продукцію або послуги, підтримувати конкурентоспроможну позицію та управляти інформацією.

Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, or ethical standards. Compliance risk exposes the institution to fines, payment of damages, and the voiding of contracts.	Ризик недотримання правил – це наявний або потенційний ризик для надходжень та капіталу, який виникає через порушення або недотримання банком вимог законів, нормативно-правових актів або етичних норм. Цей ризик може призвести до сплати штрафних санкцій, грошового відшкодування збитків та скасування контракту.
Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.	Стратегічний ризик – це наявний або потенційний ризик для надходжень та капіталу, який виникає через неправильні управлінські рішення, неналежну реалізацію рішень і відсутність реагування на зміни в бізнес-середовищі.
Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services. This risk may expose the institution to litigation, financial loss, or a decline in its customer base.	Ризик репутації – це наявний або потенційний ризик для надходжень та капіталу, який виникає через негативне сприйняття іміджу фінансової установи громадською думкою. Це впливає на здатність банку встановлювати нові відносини або надавати нові послуги. Цей ризик може втягнути установу у судову тяжбу або спричинити фінансові втрати та скорочення основної бази клієнтів.

Module 9. Modern banking for older people

Ex 9.1. Pre-reading: answer the questions:

1. What do you think, do older people really need New user-friendly technology? Why?
2. What new methods which make life for older people easier do you know?

Ex 9.2. Read the text

Modern banking for older people

New **user-friendly technology** needs to be developed to help older people access modern banking methods, argue the researchers behind a new government-sponsored project.

Many older people are wary of **ATM cards** and internet banking

Many bank teams are working to help the nearly 2.4m people over the age of 80 in the UK to become more comfortable with **digital banking**.

Their aim will be to develop **assistive technology** for older people who feel uneasiness with internet banking or chip and pin cards. An even greater focus will be on members of the elderly community without a banking account.

Many older people who do not have a traditional bank account, have a special Post Office account, which allows pensioners to **withdraw money** from a staff member at the counter.

These accounts require pensioners to withdraw large sums of cash at once and are not much better than having no account at all. They're in a difficult position for **financial abuse**.

The new assistive technology will be tried out by a variety of focus groups over 18 months.

Some ideas include a wallet shaped **foldable display**. One half would display recent transactions with dates and amounts, the other half your current balance, as a figure and an analogue quantity.

One of the main problems are means for identifying oneself because many older people have trouble remembering passwords and PINs.

Assistive technology designed for these issues have already been deployed in several countries. Banks announced plans to ramp up installations of biometric ATMs, which enable older people to access their bank accounts with a **thumb impression** instead of a PIN.

The system works by scanning a fingerprint of a customer when they open an account. **A template** of the fingerprint is stored in the customer's cash card. After inserting the card into the machine, the customer's fingerprint is captured with a built-in scanner and compared with the stored impression.

Aside from cash machines, there will need to be more work done to make online banking more accessible. Older people weren't forced to use computers when they were at work unlike the baby boomers. So the notions like menus and passwords are very foreign to them.

Efforts to make modern banking methods more attractive and accessible to older people are warmly welcomed. However, it is important that alternatives continue to be made available to older people who are unable to use modern banking methods such as internet banking and chip and PIN. For example, improving internet banking systems will be little help to the third of people over 65 who have never even used the internet.

These technologies are believed to be able to become a big enabler for making older people more comfortable with modern banking, and the goal of their research will be to deploy the solutions they think work best.

Ex 9.3. Answer the following questions

1. Why does new user-friendly technology need to be developed?
2. What will be the aim of many bank teams?
3. What do many older people have instead of a traditional bank account?
4. What do these accounts require?
5. What do installations of biometric ATMs enable older people to access?
6. What are the advantages of these technologies?

Ex 9.4. Match the following definitions

a) user-friendly technology	1) дисплей, що складається
b) digital banking	2) картка для використання в банкоматах
c) assistive technology	3) фінансове зловживання
d) withdraw the cash	4) відбиток великого пальця
e) financial abuse	5) зростати
f) foldable display	6) легка у використанні технологія
g) ramp up	7) цифрові банківські операції

h) thumb impression	8) допоміжна технологія
i) ATM cards	9) знімати гроші
j) template	10) зразок

Ex 9.5. Complete the following sentences from the words from the box

ramp up, thumb impression, financial abuse, withdraw, assistive technology, digital banking, user-friendly technology

1. New …… …… …… needs to be developed to help older people access modern banking methods, argue the researchers behind a new government-sponsored project.
2. Many bank teams are working to help the nearly 2.4m people over the age of 80 in the UK to become more comfortable with …… ……...
3. Their aim will be to develop …… ……for older people who feel uneasiness with internet banking or chip and pin cards.
4. These accounts require pensioners to …… large sums of cash at once and are not much better than having no account at all. They're in a difficult position for …… ……..
5. Banks announced plans to …… …… installations of biometric ATMs, which enable older people to access their bank accounts with a …… …….. instead of a PIN.

Ex 9.6. Insert the prepositions

of, with, from, out, for, up

1. Many older people are wary …. ATM cards and internet banking
2. Many bank teams are working to help the nearly 2.4m people over the age of 80 in the UK to become more comfortable…. digital banking.
3. Many older people who do not have a traditional bank account, have a special Post Office account, which allows pensioners to withdraw money ….. a staff member at the counter.
4. The new assistive technology will be tried … by a variety of focus groups over 18 months.
5. Assistive technology designed… these issues have already been deployed in several countries.
6. Banks announced plans to ramp … installations of biometric ATMs, which enable older people to access their bank accounts with a thumb impression instead of a PIN.
7. After inserting the card into the machine, the customer's fingerprint is captured …. a built-in scanner and compared with the stored impression.

Ex 9.7. Here are the answers. Work out the questions

1. New user-friendly technology needs to be developed to help older people access modern banking methods.

2. The aim will be to develop assistive technology for older people who feel uneasiness with internet banking or chip and pin cards. An even greater focus will be on members of the elderly community without a banking account.

3. These accounts require pensioners to withdraw large sums of cash at once and are not much better than having no account at all.

4. One of the main problems are means for identifying oneself because many older people have trouble remembering passwords and PINs.

5. Assistive technology works by scanning a fingerprint of a customer when they open an account. A template of the fingerprint is stored in the customer's cash card. After inserting the card into the machine, the customer's fingerprint is captured with a built-in scanner and compared with the stored impression.

Ex 9.8. Give the Ukrainian equivalent.

User-friendly technology; digital banking; assistive technology; withdraw the cash; financial abuse; foldable display; to ramp up; thumb impression; ATM cards.

Ex 9.9. Give the English equivalent.

Дисплей, що складається; кредитні картки; фінансове зловживання; сканування відбитку пальця; зростати; легка у використанні технологія; цифрова банківська справа; допоміжна технологія; знімати гроші; зразок (відбитку пальця).

Ex 9.10. Translate sentences into English

1. Багато літніх людей підозріло ставляться до використання кредитних карток та послуг інтернет-банкінгу. 2. Багато груп дослідників працюють, щоб допомогти майже 2,4 млн. людей користуватися послугами цифрового банкінгу. 3. Пенсіонери вимушені знімати великі суми грошей з рахунку. 4. Пенсіонери знаходяться у складному становищі через фінансові зловживання. 5. Одна із ідей – створити дисплей, що складається у формі гаманця. 6. Банки заявили, що планують збільшити видачу біометричних кредитних карток. 7. Літні люди будуть мати доступ до своїх рахунків за допомогою сканування відбитка пальця замість введення пін-коду. 8. Система працює таким чином: сканується відбиток пальця, коли клієнт відкриває рахунок. 9. Новітні та легкі у використанні технології допоможуть літнім людям мати доступ до сучасних банківських операцій.

Ex 9.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

New user-friendly technology needs to be developed to help older people access modern banking methods.	Потрібно розробляти новітні та легкі у використанні технології для того, щоб допомогти літнім людям мати доступ до сучасних банківських

	операцій.
Many older people are wary of ATM cards and internet banking.	Багато літніх людей підозріло ставляться до використання кредитних карток та послуг інтернет банкінгу.
Many bank teams are working to help the nearly 2,4m people over the age of 80 in the UK to become more comfortable with digital banking.	У Великій Британії багато груп банківських службовців працюють над тим, щоб допомогти майже 2,4 млн. людей у віці понад 80 років з комфортом користуватися послугами цифрового банкінгу.
Their aim will be to develop assistive technology for older people who feel uneasiness with internet banking or chip and pin cards.	Їх головна мета – розробити допоміжні технології для літніх людей, які відчувають труднощі при використанні послуг інтернет-банкінгу, чіпів або пін-карт.
Many older people who do not have a traditional bank account, have a special Post Office account, which allows pensioners to withdraw money from a staff member at the counter.	Багато літніх людей не мають традиційного банківського рахунку, але мають спеціальний поштовий рахунок, який надає можливість пенсіонерам отримувати гроші у касі банку.
These accounts require pensioners to withdraw large sums of cash at once and are not much better than having no account at all. They're in a difficult position for financial abuse.	Пенсіонери вимушені одноразово знімати великі суми грошей з поштового рахунку, що є не набагато краще, ніж не мати рахунку зовсім. Пенсіонери знаходяться у складному становищі через ризик фінансового зловживання.
The new assistive technology will be tried out by a variety of focus groups.	Нові допоміжні технології будуть випробувані на різноманітних групах людей.
Some ideas include a wallet shaped foldable display. One half would display recent transactions with dates and amounts, the other half your current balance, as a figure and an analogue quantity.	Одна із ідей – створити дисплей, що складається у формі гаманця. Одна половина буде відображати нещодавні операції з датами та сумами, інша – поточний баланс у цифрах та аналоговій кількості.
One of the main problems are means for identifying oneself because many older people have trouble remembering passwords and PINs.	Одна з найголовніших проблем – це спосіб підтвердження особи, тому що багато літніх людей мають труднощі із запам'ятанням паролів та пін-кодів.

Assistive technology designed for these issues have already been deployed in several countries. Banks announced plans to ramp up installations of biometric ATMs, which enable older people to access their bank accounts with a thumb impression instead of a PIN.	Допоміжна технологія, розроблена для вирішення саме таких питань, була введена у декількох країнах. Банки заявили, що планують збільшити встановлення біометричних банкоматів, які нададуть можливість літнім людям мати доступ до їх рахунків за допомогою сканування відбитка пальця замість введення пін-коду.
The system works by scanning a fingerprint of a customer when they open an account. Aside from cash machines, there will need to be more work done to make online banking more accessible.	Система працює за допомогою сканування відбитку пальця, коли клієнт відкриває рахунок. Окрім банкоматів, потрібно виконати багато роботи, щоб зробити онлайн-банкінг більш доступним.
These technologies are believed to be able to become a big enabler for making older people more comfortable with modern banking, and the goal of their research will be to deploy the solutions they think work best.	Вважають, що ці технології дуже допоможуть літнім людям використовувати зручні сучасні послуги банкінгу. Головна мета банківських досліджень – ввести у дію такі прилади, які, на їх думку, працюють найкраще.

Module 10. Identity Control

Ex 10.1. Pre-reading: answer the questions:

1. Have you ever been a victim of bank fraud?
2. Do you think most banks have a reliable fraud security nowadays?

Ex 10.2. Read and translate the text

Identity Control

With anti-money laundering and Know Your Customer regulations and increasing competition, identification control is a central issue for the future. Imagine waking up one morning to find that your identity has been taken over by someone who has destroyed your credit rating, damaged your personal credibility and taken control of what you need to continue with your normal everyday life. And the nightmare may not end when the perpetrator is apprehended.

It is now common for identity theft to persist after the criminal has been caught — there have been cases in the US where fraudsters were able to continue to use identity details while in prison. In this respect, identity theft is comparable to a serious personal or physical attack with victims saying "I thought I would never get them out of my life". One aspect of identity management is reducing fraud losses and protecting banks' customers.

Fraud is a "time bomb waiting to happen" from a customer service perspective. The banks have been slow to move on prevention measures because the financial losses from fraud have been relatively low and the return on investment isn't there. Yet identity theft is undercutting customers' trust in banks because of its personal nature and growing prevalence.

While the introduction of technologies like Chip and PIN are reducing credit/debit card fraud, this has pushed the fraudsters online and they are becoming more creative in developing ways to obtain personal information. Common tactics include phishing, such as sending emails claiming to be from a bank asking for personal and security information, and Trojans, which are installed on a customer's PC and records security and log-in details.

Compounding the problem, the big banks are sending out the wrong messages to their customers regarding online fraud. What the banks are finding is that customers have a reluctance to do business online because of the perceived risk of fraud. So the major stakeholders have come out to say that the market at the moment isn't secure online and because of that they are not getting the take-up on the online channels.

Most banks are still grappling with finding the right technology at the right price and the right ease of use for their customers. Identity management is also about proving to the financial services regulators that the institution is complying with regulations, such as Know Your Customer and Anti-Money Laundering. The big challenge for financial institutions is creating an identity management system that can determine that someone is who they say they are and where they say they are.

Identity verification is considered as a critical element of a remittance service. In order to initiate a funds transfer transaction you need to know your customer and make sure that the purpose of the payment is a legitimate purpose, that there isn't any money laundering. So there are a variety of controls and risk mitigates that banks have put in place for any sort of funds transfers. There is regulatory screenings, such as know your customer and due diligence on account opening, and ID verification is really another form of this process. This is no different from what banks have been doing for many years. Citigroup offers a wholesale outsourcing service to other banks or remittance service providers, which includes a technology solution to capture the appropriate fields of identity information of the remitter for each country and then sends it off to an independent agent or third party for verification in compliance with the KYC and anti-money laundering regulations.

A number of security vendors create profiles of end-user behaviour as part of their identity management systems to dive deeper into KYC. To create a profile, the system monitors every customer interaction, then starts to build a picture of each customer's normal pattern and uses that to detect when that customer goes out of that pattern. Having a greater understanding of who each customer is can benefit a financial institution by creating a better, more unified customer identity regardless of the channel by which they are communicating.

Some product managers point to an increasing level of cross-channel phishing, where the fraudsters exploit the loopholes between two channels. The business sense of creating a unified view of the customer is clear. To be able to unify your view of a particular person or a particular identity — given that is could be a fraudster who has hijacked that identity — you need to get a common view as to their behaviour, what they are doing, where they are doing it, did they just withdraw money from their internet bank account and then call telephone banking and try to transfer money and

those types of things. So the more you can unify that experience, the more you can automate the process of tracking and detecting potentially fraudulent behaviour.

Richard Baker, IT management consultant, outlines the effect that the Single Euro Payments Area will have on identity management. "There is an industry requirement to move to real-time clearance in October 2007. The reason that strong authentication becomes important there, and particularly not just authentication of access to the website but also the authentication of transactions, is that because the transaction will happen in real-time and the money will move in real-time, the banks will actually lose that window they have got to check for fraudulent behaviour before the transaction takes place."

"If you look at the popular press, they complain about the three day window and three days of interest that the banks are making, but what they don't actually talk about is that the banks are using those three days to track fraudulent transactions. They are not going to have that opportunity in the future because the money will have already moved. If it moves in real-time then it can move from the recipient bank as well. The fraudsters could get the money far away quite quickly and so there isn't much opportunity to reverse the transaction," he says.

Banks are facing an operational issue that slows their ability to create an end-to-end unified experience on different channels and across disparate networks. Historically, financial institutions are structured around silos with expertise in those different channels. A global architecture team is needed who are worried about security and will struggle to bring this together in a cohesive strategy across those channels. Another issue is the trend towards consolidation in the banking industry, with highly acquisitive banks such as Santander or UniCredit, making the possibility of creating the unified identity management infrastructure incredibly tricky.

Many believe that this is leaving room for non-bank competitors that don't have the same legacy systems.

Ex 10.3. Answer the questions:

1. What are the difficulties connected with fraud cases?
2. What are the common tactics of fraudsters?
3. What has become a challenge for financial institutions now?
4. What is the reason for strong authentication to become important?
5. What is necessary for solving fraud problems?

Ex 10.4. Match the Ukrainian translations to the English phrases:

a) identity theft	1) зменшення втрат внаслідок шахрайств
b) reducing fraud losses	2) заходи щодо попередження
c) prevention measures	3) Єдина Європейська Платіжна Зона
d) identity verification	4) послуга переказу грошей
e) remittance service	5) перехресний фішінг
f) anti-money laundering regulations	6) поведінка кінцевих користувачів
	7) крадіжка чужої ідентичності

g) end-user behaviour h) cross-channel phishing i) fraudulent behaviour j) Single Euro Payments Area	8) перевірка особистих даних 9) боротьба з відмиванням коштів 10) шахрайські дії

Ex 10.5. Complete the following sentences from the words in the box

reducing fraud losses, prevention measures, identity, end-user behaviour, cross-channel phishing, financial institutions, legacy systems

1. One aspect of identity management is …….. and protecting banks' customers.
2. The banks have been slow to move on …… because the financial losses from fraud have been relatively low.
3. The big challenge for financial institutions is creating an …….. management system.
4. A number of security vendors, create profiles of …… as part of their identity management systems.
5. Some product managers point to an increasing level of …….
6. Historically, ……. are structured around silos with expertise in those different channels.
7. Many believe that this is leaving room for non-bank competitors that don't have the same ……..

Ex 10.6. Insert the prepositions

for, from, of, with, to

1. It is now common ….. identity theft to persist after the criminal has been caught.
2. Fraud is a "time bomb waiting to happen" ….. a customer service perspective.
3. Most banks are still grappling with finding the right technology at the right price and the right ease ….. use for their customers.
4. Historically, financial institutions are structured around silos ….. expertise in those different channels.
5. A global architecture team is needed who will struggle ….. bring this together in a cohesive strategy across those channels.

Ex 10.7. Here are the answers. Work out the questions.

1. Identity theft is comparable to a serious personal or physical attack.
2. Identity theft is undercutting customers' trust in banks because of its personal nature and growing prevalence.
3. What the banks are finding is that customers have a reluctance to do business online because of the perceived risk of fraud.
4. Identity verification is considered as a critical element of a remittance service

5. To be able to unify your view of a particular person or a particular identity – given that is could be a fraudster who has hijacked that identity – you need to get a common view as to their behaviour.

6. The reason that strong authentication becomes important there, and particularly not just authentication of access to the website but also the authentication of transactions, is that because the transaction will happen in real-time.

Ex 10.8. Match words in the columns below

a) Identity	1) cheat
b) reducing	2) restraint
c) fraud	3) acting
d) prevention	4) damping
e) verification	5) upkeep
f) remittance	6) order
g) laundering	7) control
h) regulation	8) cleaning
i) behaviour	9) assurance

Ex 10.9. Translate into Ukrainian

Verification; remittance; identity; anti-money laundering regulations; end-user behaviour; financial institutions; cross-channel phishing; reducing; competitor.

Ex 10.10. Translate into English

Заходи щодо попередження; зменшення; шахрайство; Єдина Європейська Платіжна Зона; послуга переказу грошей; перехресний фішінг; кінцевий користувач; викрадач особистості; ідентифікація; боротьба з відмиванням коштів; шахрайські дії.

Ex 10.11. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

With anti-money laundering and Know Your Customer regulations and increasing competition, Identity verification is a central issue for the future. Imagine waking up one morning to find that your identity has been taken over by someone who has destroyed your credit rating, damaged your personal credibility and taken control of what you need to continue with your normal everyday life. And the nightmare may not end when the	Контроль ідентифікації та боротьба з відмиванням грошей в умовах зростаючої конкуренції є одним з ключових моментів у майбутньому. Уявіть собі, що, прокинувшись одного разу вранці, ви виявляєте, що Ваша ідентичність була кимось вкрадена, хтось знищив Ваш кредитний рейтинг, зруйнував довіру до Вас як до особистості і перебрав контроль над вашим повсякденним життям. І жах ще не закінчиться, коли

perpetrator is apprehended.	зловмисника буде спіймано.
It is now common for identity theft to persist after the criminal has been caught — there have been cases in the US where fraudsters were able to continue to use identity details while in prison. In this respect, identity theft is comparable to a serious personal or physical attack with victims saying "I thought I would never get them out of my life". One aspect of identity management is reducing fraud losses and protecting banks' customers.	Зараз вже є випадки, коли крадії ідентичності продовжують свою діяльність після того, як їх було спіймано. У США були випадки, коли шахраї використовували персональні дані людей, вже знаходячись у в'язниці. У цьому розумінні викрадення ідентичності можна порівняти з небезпечним фізичним нападом на жертву, яка потім каже: «Я гадав, що не зможу від них позбавитись». Один з аспектів контролю ідентифікації – це захист клієнта банку і зменшення кількості шахрайств.
Fraud is a "time bomb waiting to happen" from a customer service perspective. The banks have been slow to move on prevention measures because the financial losses from fraud have been relatively low and the return on investment isn't there. Yet identity theft is undercutting customers' trust in banks because of its personal nature and growing prevalence.	Шахрайство – це бомба сповільненої дії в обслуговуванні клієнта. Таке може трапитися з кожним клієнтом. Але банки не дуже поспішають вводити системи, які протидіють шахрайству у зв'язку з порівняно невеликими втратами від нього та тим, що це не стосується прибутку. Однак викрадачі чужої ідентичності підривають довіру клієнтів до банку через те, що це стосується їх особисто.
While the introduction of technologies like Chip and PIN are reducing credit/debit card fraud, this has pushed the fraudsters online and they are becoming more creative in developing ways to obtain personal information. Common tactics include phishing, such as sending emails claiming to be from a bank asking for personal and security information, and Trojans, which are installed on a customer's PC and records security and log-in details.	Введення таких технологій, як чіп та пін, зменшило кількість шахрайств з кредитними картками. Але воно підштовхнуло шахраїв до більшої винахідливості в пошуках шляхів одержання інформації за допомогою інтернету. Зазвичай для цього використовують такі методи, як фішінг – відправка листів начебто від імені банку із запитом про особисту і секретну інформацію та трояни – віруси, що встановлюються на комп'ютери клієнтів і записують інформацію, руйнуючи безпеку.

Identity verification is considered as a critical element of a remittance service. In order to initiate a funds transfer transaction you need to know your customer and make sure that the purpose of the payment is a legitimate purpose, that there isn't any money laundering. So there are a variety of controls and risk mitigates that banks have put in place for any sort of funds transfers. There is regulatory screenings, such as know your customer and due diligence on account opening, and ID verification is really another form of this process. This is no different from what banks have been doing for many years. Some banks offer a wholesale outsourcing service to other banks or remittance service providers, which includes a technology solution to capture the appropriate fields of identity information of the remitter for each country and then sends it off to an independent agent or third party for verification in compliance with the KYC (Known Your Customer) and anti-money laundering regulations.	Перевірка особистості є вирішальним елементом переказу грошових коштів. Для того, щоб ініціювати переказ грошових коштів, ви повинні знати свого клієнта і переконатися, що мета сплати законна, що це не відмивання грошей. Таким чином, існує ціла низка заходів контролю та зниження ризиків, які створили банки для будь-якого виду грошових переказів. Так, є методи відсіювання, такі як «Знай Свого Клієнта» (ЗСК) і належна обачливість при відкритті рахунку. Перевірка ідентифікації – це ще один метод у цьому процесі. Все це не відрізняється від того, що робили банки впродовж багатьох років. Деякі банки пропонують оптові аутсорсингові послуги іншим банкам або переказ грошей провайдерам, що передбачає технологічні рішення зі збору відповідної інформації про особистість платника для кожної країни. Після цього її відправляють незалежному агенту або третій стороні для перевірки відповідності вимогам системи ЗСК (Знай Свого Клієнта) та тим, що стосуються боротьби з відмиванням коштів.
A number of security vendors, create profiles of end-user behaviour as part of their identity management systems to dive deeper into KYC. To create a profile, the system monitors every customer interaction, then starts to build a picture of each customer's normal pattern and uses that to detect when that customer goes out of that pattern.	Чимало продавців систем безпеки створюють профілі поведінки кінцевих користувачів як частину своєї системи керування ідентифікацією для втілення принципу «Знай Свого Клієнта». Щоб створити профіль, система контролює всі дії користувачів, потім будується картина звичної схеми поведінки кожного клієнта. Після цього ця схема використовується для визначення того, коли клієнт виходить за її межі.
Some product managers point to an increasing level of cross-channel	Деякі менеджери вказують на зростаючий рівень перехресного

phishing, where the fraudsters exploit the loopholes between two channels. The business sense of creating a unified view of the customer is clear. To be able to unify your view of a particular person or a particular identity — given that is could be a fraudster who has hijacked that identity — you need to get a common view as to their behaviour, what they are doing, where they are doing it, did they just withdraw money from their internet bank account and then call telephone banking and try to transfer money and those types of things. So the more you can unify that experience, the more you can automate the process of tracking and detecting potentially fraudulent behaviour.	фішінгу, коли шахраї використовують шпаринки між двома каналами. Мета створення єдиної концепції замовника зрозуміла. Щоб уніфікувати ваше уявлення про конкретну людину або конкретну особистість – бо це може бути шахрай, який викрав чужу ідентичність, – ви повинні отримати загальне уявлення про поведінку клієнтів: що вони роблять, де вони це роблять, чи вони просто зняли гроші зі свого банківського рахунку через Інтернет, а потім телефонують і намагаються переказати гроші і т. ін. Таким чином, чим краще ви зможете об'єднати ці прояви, тим краще ви зможете автоматизувати процес відслідковування та виявлення потенційно шахрайських дій.
Some IT management consultants outline the effect that the Single Euro Payments Area will have on identity management. The reason that strong authentication becomes important there, and particularly not just authentication of access to the website but also the authentication of transactions, is that because the transaction will happen in real-time and the money will move in real-time, the banks will actually lose that window they have got to check for fraudulent behaviour before the transaction takes place."	Деякі IT консультанти описують ефект, який буде мати Єдина Європейська Платіжна Зона на контроль ідентифікації. Причиною того, що надійна аутентифікація стає важливою не тільки під час доступу до сайту, але і для окремих транзакцій, є те, що угоди укладаються в режимі реального часу, і гроші теж обертаються в реальному часі. Таким чином, банки фактично втрачають те вікно, яке вони мали для перевірки шахрайських дій раніше, ніж пройде операція.
Banks are facing an operational issue that slows their ability to create an end-to-end unified experience on different channels and across disparate networks. A global architecture team is needed who are worried about security and will struggle to bring this together in a cohesive strategy across those channels	Банки стикаються з різноманітними операційними діями, які сповільнюють їх здатність створювати уніфіковану схему дій від початку до кінця по різних каналах і через різні мережі. Необхідна об'єднана команда, яка б турбувалася про заходи безпеки і відпрацьовувала послідовну стратегію дій по всіх мережах.

Module 11. Unseen Cyber-Threats

Ex 11.1. Pre-reading. Answer the following questions:

1. Have you ever encountered cyber-threats which you could not cope with yourself?
2. Can you give an example of a cyber attack covered in mass media?

Ex 11.2. Read the text and look up the new words

Unseen Cyber-Threats

Security experts are seeing an increase lately in advanced persistent threats, threats that have no known signature or known pattern of behavior.

"The first victim is patient zero," note many **cyber** lead executives. These **threats lurk** unseen in servers, applications and databases and are very difficult to detect. They often are created by nation-states or companies **affiliated with** them, they can change their own appearance and migrate from server to server seeking confidential information, they can establish communication with their creators, and they can wait stealthily and patiently until conditions are just right to attack.

These thieves are after not just bank or card account information, but intellectual property, such as product development or marketing plans and corporate strategy. This information is valuable not only to an economic competitor but to a nation-state that has some kind of relationship with companies that owe sovereign **allegiance** to that government.

The value of research and development in the U.S. was estimated at $4 billion, about 2.8 % of the nation's **gross domestic product**. If somebody were to steal that, they would get all of the benefit and not have to pay any of the cost.

One senior banker said, “Why would the Chinese hack me? I have their money, they want me to secure their money. They're not going to steal their own money.”

In fact, banks, credit unions and insurance companies are among the most **coveted targets**. First off, they have a broad base of customers; someone executing a

social engineering trick can play the numbers and send out the email to millions of email subscribers. The bad guys are following the money to financial institutions and looking for ways to get users to compromise their credentials or the institution itself to open a place where they can further **perpetuate their crimes**.

Origins of the apt attack

The term "**advanced persistent threat**" evolved from the U.S. military and originally was used as a cover name for Chinese hacking. It has since evolved to describe a type of attack that meets the definition: advanced in that it's very sophisticated in the technical abilities of the attackers, persistent in that it keeps coming back - it's so well-resourced that it has the time and money to keep plugging away when they want **to penetrate** an organization. And it's generally associated with a nation-state attack.

Advanced persistent attacks put **sophisticated malware** on a company's systems through a social engineering-phishing type attack approach, with incredible persistence and detail. A country might dedicate 100,000 people to such a project, who will build detailed personal profiles on individuals they're going after.

The malware learns about **vulnerabilities** inside a company's systems, collects intelligence, and seeks intellectual property or sensitive data. It has the potential to encrypt that information, copy it and send it out at night when it's less noticeable.

These cleverly crafted pieces of malware know how to morph in such a way to not to **be detected**, and they can establish a **morphing schedule** so they morph faster than a signature could catch up to them. One example of this type of malware was the Zeus banking Trojan that Microsoft's crime unit worked with law enforcement to catch.

That malware was so sophisticated that it would act as that man in the middle and display actual account balances on a page that looked so unbelievably real, users had no idea what was going on.

Some observers thought it was odd that Microsoft participated in the raid. However, Microsoft has a **vested** interest in going after such perpetrators and protecting its own interests abroad.

Preventing attacks

The loss of intellectual property can have several effects. If somebody steals your intellectual property and they can introduce your product to the market and make it more cheaply, the value of your investment is infinitely **demonetized**. Your adversary gets all of the return and pays none of the investment. Secondly, the IP thief may not be able to produce the product at the level of quality that the originating firm does, so the firm's reputation may be damaged.

Banks should consider the real and likely scenario that they've already been hacked and that some or all of their systems are owned. They have a long-term **vulnerability** and they need to look at the entire ecosystem of layered defense - having technical solutions in place that provide perimeter and endpoint security.

To protect themselves, banks need to do continuous monitoring from within. Having a single firewall is not sufficient any more. You have to constantly monitor for changes in your system, and then find a way to collect and remove the **malware** from your system.

Companies also need to establish a deliberate strategy to protect their most sensitive information. If a company uses **proprietary algorithms** for market trading, those need to be treated specially and the access to those controls has to be done in such a way that it's more difficult for those potential **malware** instances to get to it.

Knowing what's going on in your networks is critical. The perpetrators of these attacks are **sophisticated** and have access to commercial antivirus tools, and the applications and architectures companies use.

A tactic of "**air gapping**" - ensuring that a secure network is isolated from insecure networks, such as the public Internet - can help but is not a complete answer. The Stuxnet worm, for instance, that once targeted nuclear capabilities of one country, got on the laptops of Russian contractors who supported those systems through thumb drives. The fact that something isn't connected to the Internet does not necessarily mean that malware cannot get on those systems.

The FBI has recommended that computers banks use for funds transfers be dedicated to that purpose and not connected to the Internet or perform other functions. It's also specified that these **stand-alone computers** should have no active USB ports.

The Department of Defense puts hot glue in their USB ports to keep people from using them - it's a bit of a low-tech solution but effectiveness nonetheless. Such computers should ideally have no other applications on them, not even email or Microsoft Word. There's no absolute empirical evidence, but the FBI has said unofficially that companies that did this later reported that there were no incidences - the threat and opportunity had reduced to zero.

But there's no silver bullet, of course. You shouldn't assume that just because a network is isolated from the Internet, that there is no pass by which malware can infect that system or information might be stole. Insiders, insufficient discipline and lack of enforcement of policies can all open doors to attack.

Ex 11.3. Answer the following questions

1. Where do cyber-threats usually emerge? Why are they considered to be dangerous to detect?
2. What kind of information do they steal?
3. What financial institutions are among the most coveted targets?
4. How did the term “advanced persistent threat evolve”? What is the main function?
5. What is malware?
6. What kind of program can ensure the secure network?
7. What should banks do to protect against cyber-threats?

Ex 11.4. Match the following definitions

a) cyber-threats	1) слабкі місця
b) coveted targets	2) серйозна постійна загроза
c) perpetuate crime	3) бажані цілі
d) advanced persistent threat	4) проникнути
e) penetrate	5) автономні комп'ютери
f) vulnerabilities	6) наділяти
g) vest	7) ступінь безпеки, що зазвичай приймається для комп'ютерів, комп'ютерних систем або мереж, які мають бути дуже безпечними
h) adversary	8) противник
i) proprietary algorithms	9) патентовані (власні) алгоритми
j) air gapping	10) ланцюг банківських операцій, що змінюється
k) stand-alone computers	11) кіберзагрози
l) sophisticated malware	12) шкідливе та складне для розпізнання програмне забезпечення (вірус)
m) morphing schedule	13) вчиняти злочини
n) lurk	14) ховатися
o) detect	15) викрити
p) affiliate with	16) приєднатися
q) allegiance	17) відданість
r) gross domestic product.	18) валовий внутрішній продукт
s) demonetize	19) зменшувати ціну

Ex 11.5. Complete the following sentences with the words from the box

affiliate, gross domestic product, stealthily, advanced persistent threat, sophisticated malware ,coveted targets, vulnerabilities, air gapping

1. These cyber-threats often are created by nation-states or companies **…….with** them, they can change their own appearance and migrate from server to server seeking confidential information, they can establish communication with their creators, and they can wait …….. and patiently until conditions are just right to attack.

2. The value of research and development in the U.S. was estimated at $4 billion, about 2.8 % of the nation's **…….. …… …….**

3. In fact, banks, credit unions and insurance companies are among the most …… …….

4. The term "…… …… ……." evolved from the U.S. military and originally was used as a cover name for Chinese hacking.

5. Advanced persistent attacks put …… ……. on a company's systems through a social engineering-phishing type attack approach, with incredible persistence and detail.

6. The malware learns about …… inside a company's systems, collects intelligence, and seeks intellectual property or sensitive data.

7. A tactic of "…… ……." - ensuring that a secure network is isolated from insecure networks, such as the public Internet - can help but is not a complete answer.

Ex 11.6. Insert the prepositions

with, from, away, out

1. They often are created by nation-states or companies affiliated …… them, they can change their own appearance and migrate ….. server to server seeking confidential information, they can establish communication with their creators, and they can wait stealthily and patiently until conditions are just right to attack.

2. The term "advanced persistent threat" evolved …… the U.S. military and originally was used as a cover name for Chinese hacking.

3. It has since evolved to describe a type of attack that meets the definition: advanced in that it's very sophisticated in the technical abilities of the attackers, persistent in that it keeps coming back - it's so well-resourced that it has the time and money to keep plugging ……..when they want to penetrate an organization. And it's generally associated ….. a nation-state attack.

4. The malware learns about vulnerabilities inside a company's systems, collects intelligence, and seeks intellectual property or sensitive data. It has the potential to encrypt that information, copy it and send it …. at night when it's less noticeable.

5. A tactic of "air gapping" - ensuring that a secure network is isolated from insecure networks, such as the public Internet - can help but is not a complete answer.

Ex 11.7. Give the English equivalent

Слабкі місця; серйозна постійна загроза; бажані цілі; проникнути; автономні комп'ютери; наділяти; міра безпеки, що зазвичай приймається для комп'ютерів, комп'ютерних систем або мереж, які мають бути дуже безпечними; противник; патентовані (власні) алгоритми; ланцюг банківських операцій, що змінюється; кіберзагрози; шкідливе та складне для розпізнання програмне забезпечення (вірус); вчиняти злочини; ховатися; викрити; приєднатися; відданість; валовий внутрішній продукт; вилучати грошову одиницю з обороту.

Ex 11.8. Give the Ukrainian equivalent

Cyber-threats; coveted targets; perpetuate crime; advanced persistent threat; penetrate; vulnerabilities; to vest adversary; proprietary algorithms; air gapping; stand-alone computers; wait stealthily; sophisticated malware; morphing schedule; lurk; detect; affiliated with; allegiance; gross domestic product; demonetize.

Ex 11.9. Translate sentences into English

1. Шахраї шукають не лише інформацію про банківські або кредитні картки, але й інтелектуальну власність.

2. Вірус знаходить слабкі місця всередині системи компанії, збирає таємну інформацію та шукає інтелектуальну власність або секретні дані.

3. Вірус може розшифровувати інформацію, копіювати, а також пересилати її вночі, коли це менш помітно.

4. Тактика «ейр-гаппінг» гарантує ізоляцію мережі від інших небезпечних мереж.

5. Загрози з'являються раптово та непередбачувано у серверах, прикладних програмах та базах даних.

6. Такі загрози можуть мігрувати від сервера до сервера, шукаючи конфіденційну інформацію, можуть встановлювати комунікацію з їх винахідниками, а можуть терпляче чекати, поки не настануть умови, за яких можна атакувати.

7. Кредитні союзи та страхові компанії є найбажанішими цілями.

Ex 11.10. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Security experts are seeing an increase lately in advanced persistent threats. The first victim is patient zero," note many cyber lead executives. These threats lurk unseen in servers, applications and databases and are very difficult to detect. They often are created by nation-states or companies affiliated with them, they can change their own appearance and migrate from server to server seeking confidential information, they can establish communication with their creators, and they can wait stealthily and patiently until conditions are just right to attack.	Експерти з безпеки вбачають збільшення серйозних постійних загроз. Першою жертвою з них є «нульовий клієнт» – зазначають головні менеджери кіберпростору. Такі загрози з'являються раптово та непередбачувано у серверах, прикладних програмах та базах даних. Ці загрози виявити дуже важко. Зокрема, їх створюють національні організації або компанії, що пов'язані з ними. Вони видозмінюються та можуть мігрувати від сервера до сервера, шукаючи конфіденційну інформацію, встановлюють відносини з їх винахідниками, можуть терпляче чекати, поки не настануть умови, за яких можна атакувати.
These thieves are after not just bank or card account information, but intellectual property, such as product development or marketing plans and corporate strategy. In fact, banks, credit unions and insurance companies are among the most coveted targets.	Ці шахраї шукають не лише інформацію про банківські або кредитні картки, але й про створення інтелектуальної власності, такої, як розробка, удосконалення продукту або маркетингові плани та корпоративна стратегія. Насправді кредитні союзи та страхові компанії є найбажанішими

	цілями.
The term "advanced persistent threat" evolved from the U.S. military and originally was used as a cover name for Chinese hacking. Advanced persistent attacks put sophisticated malware on a company's systems through a social engineering-phishing type attack approach, with incredible persistence and detail. The malware learns about vulnerabilities inside a company's systems, collects intelligence, and seeks intellectual property or sensitive data. It has the potential to encrypt that information, copy it and send it out at night when it's less noticeable.	Термін «постійна серйозна загроза» походить з військової термінології США і спочатку використовувався як прихована назва для хакерських атак з Китаю. «Постійна серйозна загроза» упроваджує складний вірус у систему компанії через соціальний інженерно-фішінговий тип атаки з надзвичайною наполегливістю та чіткістю. Вірус вивчає слабкі місця всередині системи компанії, збирає конфіденційну інформацію та шукає інтелектуальну власність або секретні дані. Вірус може розшифровувати інформацію, копіювати, а також пересилати її вночі, коли це менш помітно.
This malware know how to morph in such a way to not to be detected.	Такий вірус знає яким чином трансформуватися, щоб ніхто не зміг його виявити.
The loss of intellectual property can have several effects. If somebody steals your intellectual property and they can introduce your product to the market and make it more cheaply, the value of your investment is infinitely demonetized. Your adversary gets all of the return and pays none of the investment. Secondly, the thief may not be able to produce the product at the level of quality that the originating firm does, so the firm's reputation may be damaged.	Втрата інтелектуальної власності може мати декілька наслідків. Якщо хтось викрадає вашу інтелектуальну власність, то вони можуть представити свій товар на ринку і зробити його дешевшим, і таким чином ціна вашої інвестиції значно зменшується. Ваш опонент отримує усі гроші, не інвестуючи нічого. І, по-друге, крадій інтелектуальної власності, можливо, не зможе створити продукт на рівні якості фірми-виробника, а внаслідок цього репутація фірми може бути зруйнована.
To protect themselves, banks need to do continuous monitoring from within. Companies also need to establish a deliberate strategy to protect their most sensitive information.	Щоб захиститися, банки мають робити постійний моніторинг зсередини. Компаніям також не завадило б встановити чітко сплановану стратегію, щоб захистити свою важливу інформацію.

Knowing what's going on in your networks is critical. The perpetrators of these attacks are sophisticated and have access to commercial antivirus tools, and the applications and architectures companies use.	Знати, що відбувається у вашій мережі – надзвичайно важливо. Злочинці, які атакують, – експерти у своїй сфері діяльності і мають доступ до комерційних антивірусних програм, прикладних програм та архітектурних схем, що використовують компанії.
A tactic of "air gapping" ensuring that a secure network is isolated from insecure networks.	Тактика «ейр-гаппінг» гарантує ізоляцію мережі від інших незахищених мереж.
The FBI has recommended that computers banks use for funds transfers be dedicated to that purpose and not connected to the Internet or perform other functions. It's also specified that these stand-alone computers should have no active USB ports.	ФБР зазначає, що банківські комп'ютери, які використовуються для перерахування грошей, повинні призначатися саме для такої мети, і не бути пов'язаними з інтернетом або виконувати інші функції. Також підкреслюється, що такі автономні комп'ютери не повинні мати активних USB портів.
The FBI has said But there's no silver bullet, of course. "You shouldn't assume that just because a network is isolated from the Internet, that there no pass by which malware can infect that system or information might be stole.	ФБР зазначила, що, звісно, не існує ідеального захисту. Треба усвідомлювати, що навіть ізольована від інтернету мережа не є повністю захищеною від можливості вірусу інфікувати систему або вкрасти інформацію.

Module 12. Crimes committed in the banking system

Ex 12.1. Pre-reading. Answer the following questions:

1. Have you ever encountered online cybercrimes?
2. How can we tackle the problem of committing cybercrimes?

Ex 12.2. Read the text and translate:

Criminal characteristic of crimes committed in the banking system by using up-to-date information technologies

Government vital activity banking system which deals with **accumulating**, dividing and using **governmental and private funds** is the most attractive for individual criminals and especially organized criminal groups. The most **financial swindles** of different kinds accomplished more often during various bank operations are committed now in this system.

Offenses committed in the banking system or by using it can be attributed to the most dangerous economic crimes since their negative influence is not only reflected on the bank itself but also the many other subjects of the economic activity and the financial system of the government at large.

The object of the **criminal trespass** depending on the kind of a crime is not the same. The criminal trespasses in the bank sphere are determined by the criminal-and-legal indication depending on the circumstances by the clauses of different chapters from the Criminal Code of Ukraine: 1.Offenses against property – "**Fraud"** (190); 2.Offenses in the sphere of economic activity – "Illegal acts with **transfer bills,** payment cards, equipment for their manufacture and other means of access to the banking accounts" (200); 3.Offenses in the sphere of using electronic computers,

systems and computer nets – “Illegal interference with the work of the electronic computers, systems and computer nets” (361); “**Larceny, misappropriation, extortion** and possession of the computer information by **swindling** or **abusing** official position” (362); “**Violation** of the operating rules for automated electronic systems”(363); (2). Funds of the government or private firms, enterprises and persons in the Ukrainian or foreign currency, goods and **property** as well are the object of these criminal trespasses.

The methods of committing banking offenses are very different. Let us examine the crimes committed by using modern information technologies: **counterfeit** and application of the plastic payments cards and computer banking information.

For the last years the Ukrainian market of the bank technologies **traversed** a path from the initial stage of computerization – realizing the most simple banking operations on the base of the personal computers, to the valuable automated banking systems, which meet the most exacting modern requirements. The international systems of payment are being introduced.

The modern state of the information systems and electronic technique allows introducing the most **delicate and interesting technologies**. One of them is so called "e-money".

The **mutual interest** of the government and the owners of the plastic cards stipulated the appearance and spread of plastic payments means. It is one of the ways for the government to **reduce the needs** in ready money mass.

The emitters recurrently inform the organizations, which accept cards, about the numbers of cards declared **null and void,** stolen, lost or **forged.** The list of the numbers of such cards is called “**stop-list**”. When using a card, it is checked for the validity of its details by the “stop-list” and with the reading unit (3).

Hackers are a real danger for the bank industry of **plastic payment means**. When using special software they can determine and then sell the numbers of **valid accounts** of the credit cards and also extend passwords, identification numbers, credit and other personal information through computer nets, thereby helping criminals to obtain illegal access to the credit offices and criminal operations with the information obtained from the electronic computers and data carriers.

But counterfeit is the most dangerous threat for the payment systems with using bank plastic cards. This kind of offenses is developed the most dynamically and creates great difficulties when researching and calculating losses. Criminals use the numbers of the valid cards and their owners even do not guess it.

Theft in the bank activity with using electronic computers or computer nets is broadly extended now. This kind of theft is characterized with that the criminals abused their official position to get unlawful access to the computer information of the financial character, concentrated in the electronic centers of the banking establishments, revealed the flaws in the activity of the inspection services and carry out the computer systems of the financial establishments.

Today there are four groups of principal means of committing computer crimes:

1. **Information piracy**: direct and electromagnetic.

2. **Unauthorized access** to information: “computer boarding”, “mystification”, “disguising”, “changeable choice”, “by tail”, “emergency”, “after fool”, “breakthrough”, “hatch”, “storehouse without walls”, “system gawks”.

3.Manipulation with information: “Trojan hobbled hoarse”, “Trojan wooden doll”, data substitution, code replacement, computer virus, “salami”, “logical bomb”, “asynchronous attack”, modeling, “kite”, “trap with bite”.

4.Obtaining and using information with criminal purpose: larceny of software, equipment by means of computer operations, theft of money by means of gaining confidential codes, **computer remittance,** manipulation with computer or introducing **alterations** to the program (4).

In the main, criminal action consists of conducting contact operations of the **wrongdoers** with the electronic computers or machine carriers, drawing necessary information or money from the e-accounts of the bank clients, possessing it or transferring it to the accounts of the “**false” organizations.**

Home and foreign researches make it possible to paint a portrait of a typical computer, electronic criminal, that is a proper profile of this social type: he is average 30 years old, by education – an engineer in the field of electronics and mathematics, or programmer, but there are some cases when the criminals never had any technical experience. Besides they are not on the books at IAA and do not have criminal past at all.

From a position of human psychophysical characteristics it is a desired official, a bright, thinking, creative person, who knows his business and is ready to accept a technical challenge. They always occupy senior posts and are equipped with special knowledge and the newest technologies, have an access to the banking computer systems.

“Hackers” – **computer rowdies** who enjoy **penetrating into** smb. else’s computer. They are capital experts on information technology. By means of telephones and home computers they are connected to the nets, which **transmit information** linked nearly with all big computers that operate in the field of economy and banking activity.

Professional criminals who act with obvious mercenary motive and have steady criminal experience are the most dangerous threat for the sphere of banking activity. Crimes that bear serial, continuous character are always concealed. More often the members of the organized criminal groups are highly skilled experts with higher mathematical, engineering and technical or economical education who are equipped with special technique. Most of the especially unsafe crimes in public offices such as misappropriation of money means to the particularly large extents committed by applying computing machinery fall on the share of this group of criminals.

Ex 12.3. Answer the following questions:

1. What are the functions of banking system?
2. How are criminal trespasses determined in the bank sphere?
3. What are the methods of committing banking offenses?

4. Why does the government consider e-money useful?
5. What are the four main methods of committing computer crimes?

Ex 12.4. Match the Ukrainian translations to the English phrases:

a) accumulating	1) фінансове шахрайство
b) governmental and private funds	2) проникати
c) financial swindle	3) кримінальне посягання
d) offense	4) взаємна зацікавленість
e) fraud	5) «чорний список»
f) transfer bills	6) державні та приватні фонди
g) larceny	7) зменшити потреби
h) misappropriation	8) збір
i) extortion	9) удосконалені технології
j) abuse	10) недійсний
k) counterfeit	11) правопорушення
l) delicate technologies	12) джерело
m) mutual interest	13) крадіжка
n) emitter	14) незаконне привласнення
o) reduce the needs	15) несанкціонований доступ
p) null and void	16) комп'ютерні хулігани
q) «stop-list»	17) вимагання
r) forge	18) шахрайство
s) computer remittance	19) рахунки переказів
t) unauthorized access	20) комп'ютерний грошовий переказ
u) computer rowdies	21) підробка
v) penetrate into smth.	22) зловживання
w) criminal trespass	23) фальсифікувати

Ex 12.5. Complete the following sentences with the words from the box

computer rowdies ,penetrating, mutual interest, reduce the needs, valid accounts ,emitters, null and void, wrongdoers, "false" organizations, accumulating, governmental and private funds, trespass, forged, financial swindles, reduce the needs

1. "Hackers" – ……who enjoy …….into smb. else's computer.
2. The object of the criminal …… depending on the kind of a crime is not the same.
3. The …… of the government and the owners of the plastic cards stipulated the appearance and spread of plastic payments means. It is one of the ways for the government to ……in ready money mass.
4. When using special software hackers can determine and then sell the numbers of ……of the credit cards.
5. The…….. recurrently inform the organizations, which accept cards, about the numbers of cards declared ……..., stolen, lost or …….

6. Criminal action consists of conducting contact operations of the ……..with the electronic computers or machine carriers, drawing necessary information or money from the e-accounts of the bank clients, possessing it or transferring it to the of the accounts of the …….

7. The most ……. of different kinds accomplished more often during various bank operations are committed now in this system.

8. Government vital activity banking system which deals with ……., dividing and using …… is the most attractive for individual criminals and especially organized criminal groups.

Ex 12.6. Insert the prepositions

from ,with ,on, into, to, of

1. The object of the criminal trespass depending …… the kind of a crime is not the same.

2. The methods …. committing banking offenses are very different.

3. For the last years the Ukrainian market of the bank technologies traversed a path ….. the initial stage of computerization

4. Obtaining and using information with criminal purpose: larceny of software, equipment by means of computer operations, theft of money by means of gaining confidential codes, computer remittance, manipulation ……. computer or introducing alterations ….. the program.

5. "Hackers" – computer rowdies who enjoy penetrating ….. smb. else's computer.

6. By means of telephones and home computers they are connected to the nets, which transmit information linked nearly …. all big computers that operate in the field of economy and banking activity.

7. Today there are four groups of principal means of committing computer crimes, one of them is unauthorized access…. information.

Ex 12.7. Here are the answers. Work out the questions.

1. Government vital activity banking system which deals with accumulating, dividing and using governmental and private funds.

2. The criminal trespasses in the bank sphere are determined by the criminal-and-legal indication depending on the circumstances by the clauses of different chapters from the Criminal Code of Ukraine.

3. The crimes committed by using modern information technologies: counterfeit and application of the plastic payments cards and computer banking information.

4. Plastic payments means is one of the ways for the government to reduce the needs in ready money mass.

5. When using special software, hackers can determine and then sell the numbers of valid accounts of the credit cards and also extend passwords, identification numbers, credit and other personal information through computer nets.

Ex 12.8. Find the synonyms

a) wrongdoer	1) to fake up
b) to counterfeit	2) source
c) emitter	3) forge
d) swindle	4) diminish
e) alteration	5) collect
f) larceny	6) change
g) extortion	7) delinquent
h) accumulate	8) permeate
i) reduce	9) thievery
j) penetrate	10) blackmail

Ex 12.9. Translate into English

Фінансове шахрайство; збір; проникати; кримінальне посягання; зловживання; підробка; комп'ютерний грошовий переказ; взаємна зацікавленість; чорний список; державні та приватні фонди; вимагання; комп'ютерні хулігани; несанкціонований доступ; недійсний; правопорушення; вимагання; крадіжка; правопорушник; неіснуючі організації.

Ex 12.10. Translate into Ukrainian

Accumulating; criminal trespass; governmental and private funds; penetrate into smth; financial swindle; computer rowdies; offense; unauthorized access; transfer bills; fraud; computer remittance; larceny; forge; abuse; counterfeit; null and void; reduce the needs; delicate technologies; emitter; "false" organizations;. draw information; conceal.

Ex 12.11. Translate sentences into Ukrainian

1. Offenses committed in the banking system or by using it can be attributed to the most dangerous economic crimes since their negative influence is not only reflected on the bank itself but also the many other subjects of the economic activity and the financial system of the government at large.
2. Funds of the government or private firms, enterprises and persons in the Ukrainian or foreign currency, goods and property as well are the object of the criminal trespasses.
3. The methods of committing banking offenses are very different.
4. For the last years the Ukrainian market of the bank technologies traversed a path from the initial stage of computerization – realizing the most simple banking operations on the base of the personal computers, to the valuable automated banking systems, which meet the most exacting modern requirements.
5. Theft in the bank activity with using electronic computers or computer nets is broadly extended now.

6. In the main, criminal action consists of conducting contact operations of the wrongdoers with the electronic computers or machine carriers, drawing necessary information or money from the e-accounts of the bank clients, possessing it or transferring it to the accounts of the "false" organizations.

7. Professional criminals who act with obvious mercenary motive and have steady criminal experience are the most dangerous threat for the sphere of banking activity.

8. Crimes that bear serial, continuous character are always concealed.

9. More often the members of the organized criminal groups are highly skilled experts with higher mathematical, engineering and technical or economical education who are equipped with special technique.

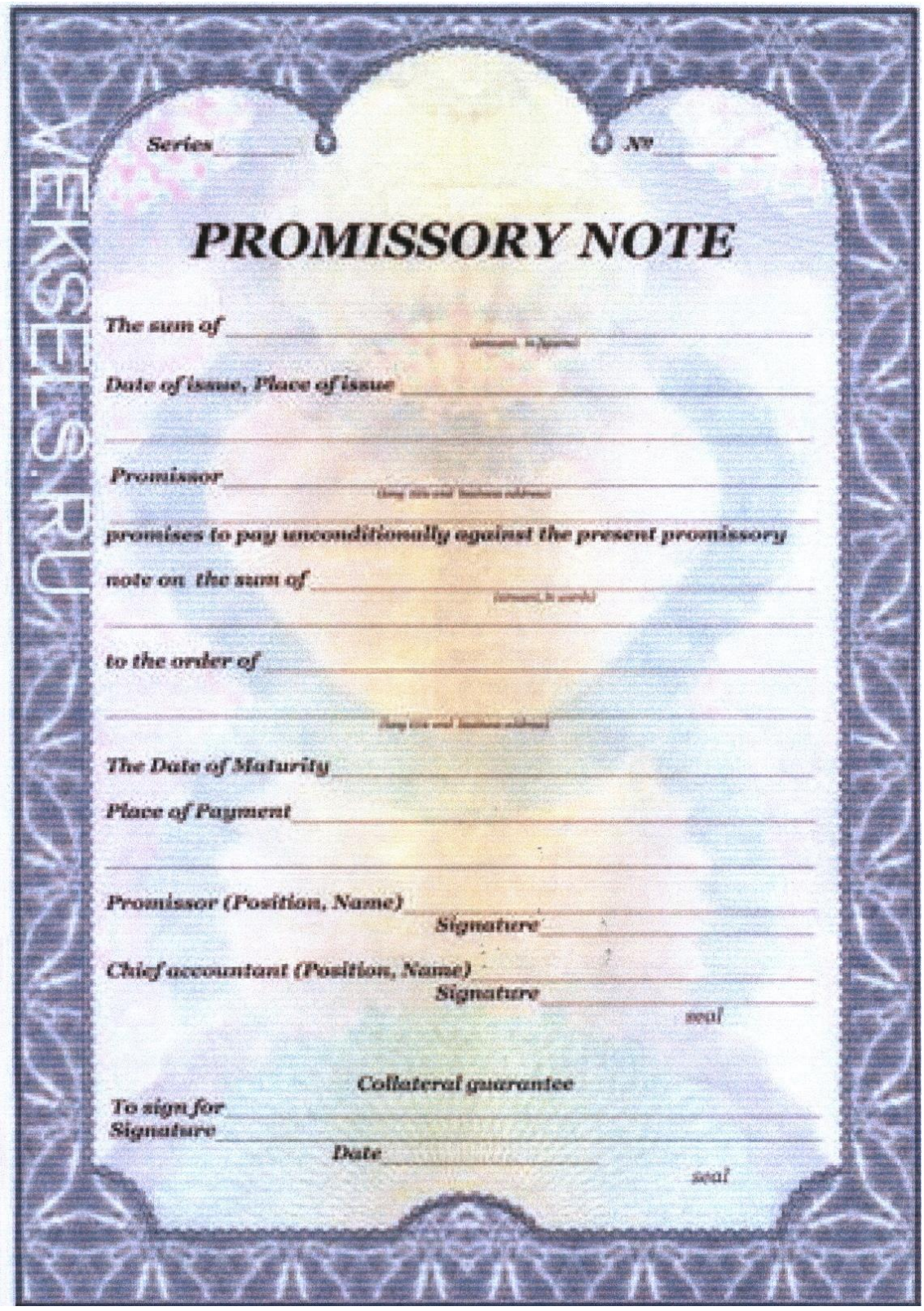
10. Most of the especially unsafe crimes in public offices such as misappropriation of money means to the particularly large extents committed by applying computing machinery fall on the share of this group of criminals.

Ex 12.12. Read the translation below, then practice English/Ukrainian and Ukrainian/English pieces by covering one part of the matching texts. If necessary, consult the covered text.

Banking system which deals with accumulating, dividing and using governmental and private funds is the most attractive for individual criminals and especially organized criminal groups.	Банківська система, яка займається збором, розподілом, використанням державних та приватних фондів, найбільш приваблива для індивідуальних злочинів, особливо організованих злочинних груп.
The most financial swindles are often committed during various bank operations. The criminal trespasses in the bank sphere are determined by the criminal-and-legal indication depending on the circumstances by the clauses of different chapters from the Criminal Code of Ukraine:	Більшість фінансових шахрайств найчастіше відбувається під час різноманітних банківських операцій. Кримінальні посягання в банківській сфері визначаються за допомогою кримінально-легальних показань залежно від обставин, обумовлених в пунктах різних статей Кримінального Кодексу України:
1. Offenses against property – "Fraud" (190);	1. Правопорушення проти власності – «Шахрайство» (ст. 190);
2. Offenses in the sphere of economic activity – "Illegal acts with transfer bills, payment cards, equipment for their manufacture and other means of access to the banking accounts" (200);	2. Правопорушення у сфері економічної діяльності – «Нелегальні акти, пов'язані з переказами грошей, картами оплати, устаткуванням для їх вироблення та іншими засобами доступу до банківських рахунків» (ст. 200);
3. Offenses in the sphere of using electronic computers, systems	3. Правопорушення у сфері використання електронних комп'ютерів,

and computer nets – "Illegal interference with the work of the electronic computers, systems and computer nets" (361);	систем, комп'ютерних мереж – «Нелегальне втручання в роботу електронних комп'ютерів, систем, і мереж» (ст. 361);
4. "Larceny, misappropriation, extortion and possession of the computer information by swindling or abusing official position" (362);	4. Крадіжка, незаконне привласнення, вимагання та володіння комп'ютерною інформацією за допомогою шахрайства або зловживання службовим становищем.
5. "Violation of the operating rules for automated electronic systems"(363);	5. Порушення правил роботи для автоматизованих електронних систем.
6. Funds of the government or private firms, enterprises and persons in the Ukrainian or foreign currency, goods and property as well are the object of these criminal trespasses.	6. Фонди державних чи приватних фірм, підприємств або фізичних та юридичних осіб, виражених у національній або іноземній валюті, товарах та власності, є об'єктами кримінального посягання.
The modern state of the information systems and electronic technique allows introducing the most delicate and interesting technologies. One of them is so called "e-money". It is one of the ways for the government to reduce the needs in ready money mass.	Сучасний стан інформаційних систем або електронних технологій дозволяє використання найбільш удосконалених та цікавих технологій. Одна з них – електронні гроші. Це є один із шляхів, яким держава зменшує потребу у готівці.
Hackers are a real danger for the bank industry of plastic payment means. Criminals use the numbers of the valid cards and their owners even do not guess it. Theft in the bank activity with using electronic computers or computer nets is broadly extended now. "Hackers" – computer rowdies who enjoy penetrating into smb. else's computer. By means of telephones and home computers they are connected to the nets, which transmit information linked nearly with all big computers that operate in the field of economy and banking activity. More often the members of	Хакери є серйозною загрозою для індустрії оплати за допомогою пластикових карт. Порушники використовують номери дійсних карт, у той час як їх власники навіть і не здогадуються про це. На сьогодні крадіжка дуже поширена у банківській сфері за допомогою використання електронних комп'ютерів та комп'ютерних мереж. «Хакери» – це комп'ютерні шахраї, які отримують задоволення, проникаючи у чужий комп'ютер. За допомогою телефонів та домашніх комп'ютерів вони поєднані з мережами, які передають інформацію, пов'язану майже з усіма головними комп'ютерами, що працюють в

the organized criminal groups are highly skilled experts with higher mathematical, engineering and technical or economical education.	економічній та банківській сфері. Найчастіше членами організованих кримінальних груп стають висококваліфіковані експерти з вищою математичною, інженерною, технічною або економічною освітою.



Series_____ № _____

PROMISSORY NOTE

The sum of _____
(amount, in figures)

Date of issue, Place of issue _____

_____

Promissor _____
(long title and business address)

_____

promises to pay unconditionally against the present promissory note on the sum of _____
(amount, in words)

_____

to the order of _____

_____
(long title and business address)

The Date of Maturity _____

Place of Payment _____

_____

Promissor (Position, Name) _____

Signature _____

Chief accountant (Position, Name) _____

Signature _____

seal

Collateral guarantee

To sign for _____

Signature _____

Date _____

seal

Ex 13.1. Study an example of a promissory note and translate it using the phrases below.

Ex 13.2. Match the Ukrainian translations to the English phrases:

a) promissory note	1) місце виплати
b) series	2) за наказом
c) the sum of	3) боржник
d) date of issue	4) зобов’язується сплатити
e) place of issue	5) ця розписка
f) promisor	6) дата видачі
g) promises to pay	7) сума
h) present promissory	8) місце видачі
i) to the order of	9) термін платежу
j) the date of maturity	10) печатка
k) place of payment	11) боргова розписка
l) seal	12) серія

Ex 13.3. Translate the sentences from Ukrainian into English, using the phrases above.

1. Дата та місце видачі вашої боргової розписки вказані на ній.
2. Боржник зобов’язується сплатити борг на суму 3000 гривень, при чому термін платежу становить 6 місяців.
3. Серія, номер, посада та підпис посадової особи є невід’ємними атрибутами боргової розписки.
4. Після того, як боргова розписка була підписана, на ній проставляються печатки.
5. Ця розписка була підписана сером Річардом Браунінгом та сером Чарльзом Вайтом.
6. Відповідно до цієї боргової розписки, міс Катаріна Олдман зобов’язується сплатити 45 000 фунтів стерлінгів серові Вікторові Роудові.
7. Дивно, але на вашій борговій розписці не вказаний термін платежу. – Можливо, це означає, що він необмежений?

Ex 13.4. Study an example of a check and then translate it, using the words, stated below.

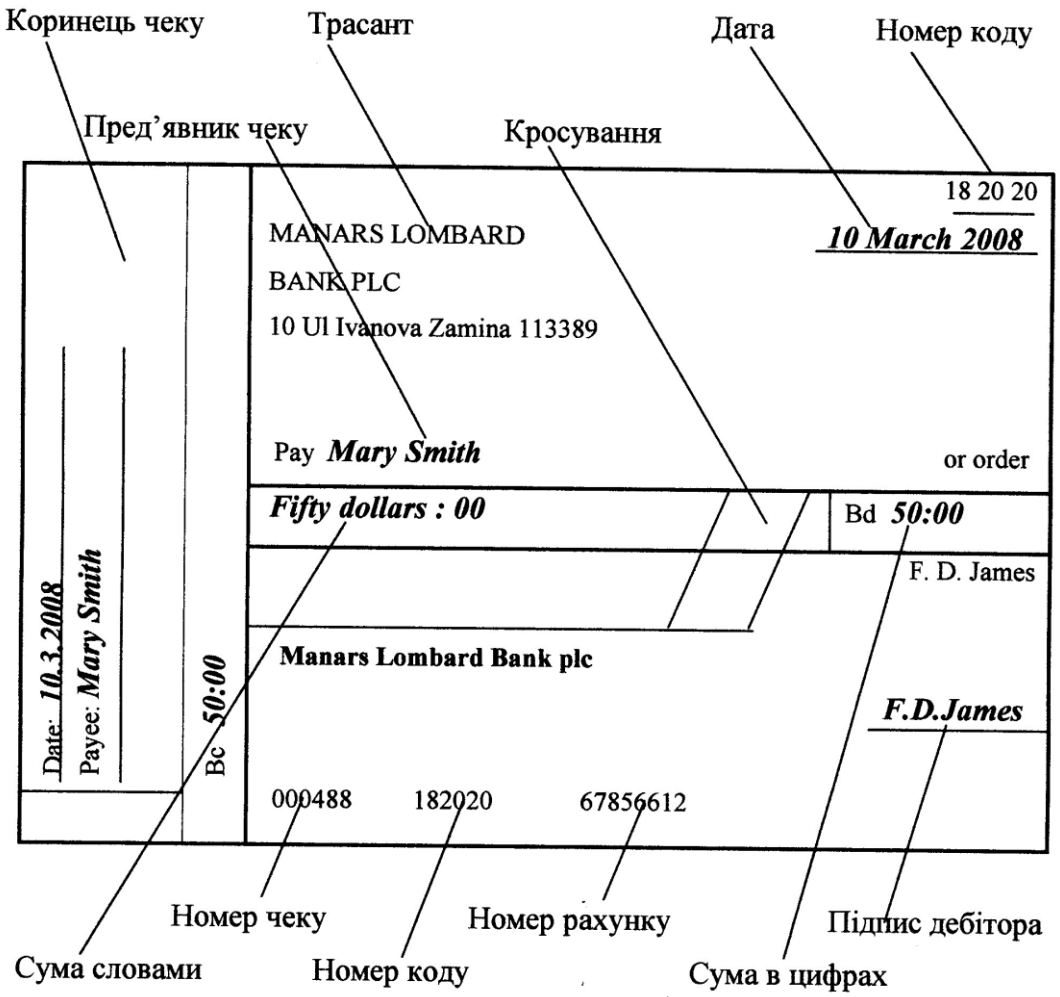


Fig. 2 An example of a check

1) корінець чеку – counterfoil;
2) пред'явник чеку – the payee;
3) трасант (банк, який виписує чек) – the drawer;
4) кросування – the crossing;
5) дата – the date;
6) номер коду – the sort code;
7) сума в цифрах – the amount in words;
8) номер чеку – the cheque number;
9) номер коду – the sort code;
10) номер рахунку – the account number;
11) сума в цифрах – the amount in figures;
12) підпис дебітора – the drawer's signature;

Ex 13.5. Translate the sentences from Ukrainian into English, using the phrases from the above list.

1. Що це за незрозумілі цифри внизу чека? – Це номер чека, номер коду та номер рахунку.

2. Яка інформація вказується на корінці чека? – Корінець чека містить дату, ім'я отримувача та суму в цифрах.

3. Пане лекторе, поясніть будь ласка, що таке кросування та трасант.

4. Навіщо на чекові має стояти підпис дебітора?
5. Яку інформацію потрібно вказувати словами? Як ви гадаєте навіщо?

Ex 13.6. Here you can find an example of a scheme of paying with check. Study it and then translate the explanation, given after it.

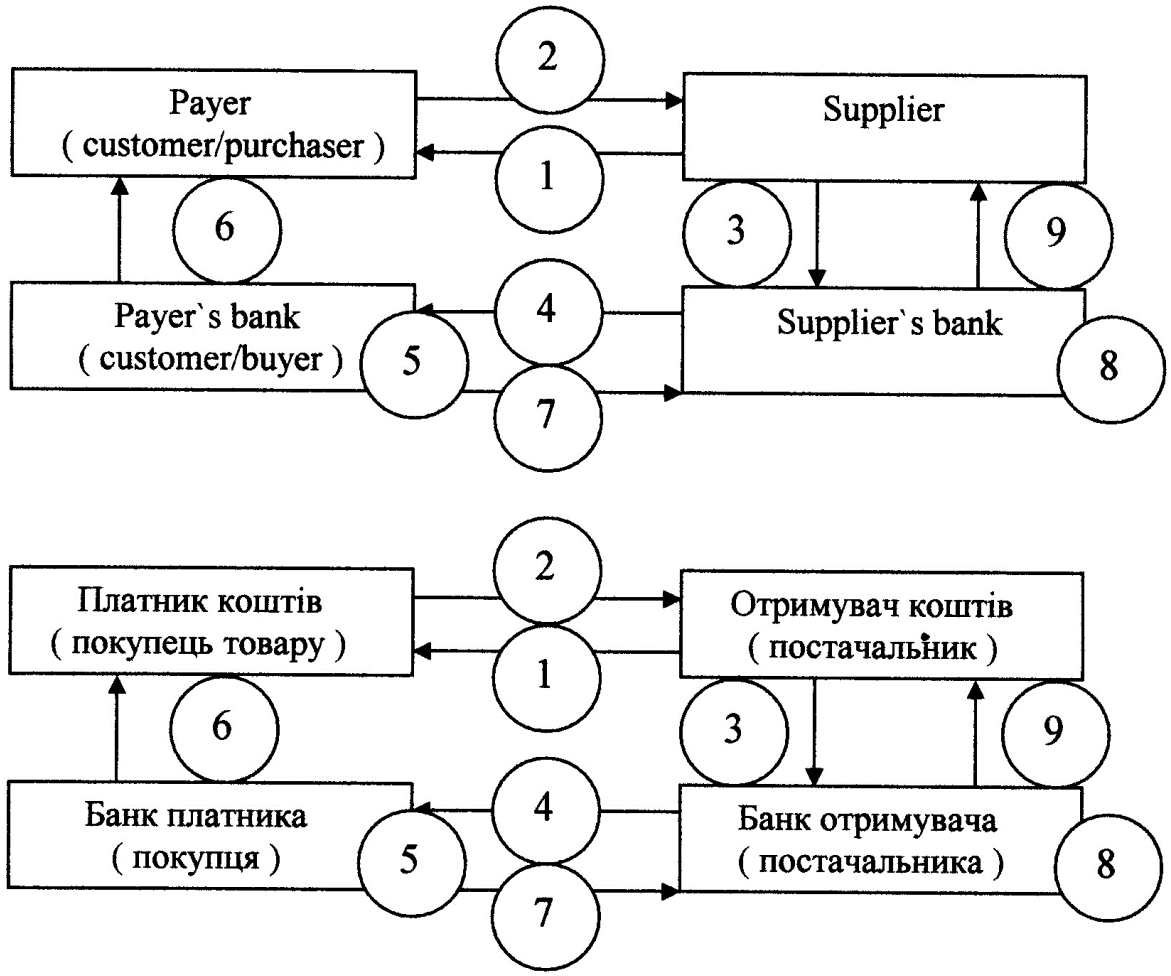


Fig. 3 An example of a scheme of paying the check

1 – постачальник (supplier) передає товар покупцеві (buyer);

2 – покупець передає чек постачальнику;

3 – постачальник передає чек у свій банк;

4 – банк постачальника направляє чек для сплати в банк покупця (payer's bank);

5 – банк платника списує (write off) кошти з рахунка (account) покупця товару;

6 – банк платника повідомляє платника про списання коштів;

7 – банк платника переказує (remittance/transfer) банку постачальника відповідні кошти;

8 – банк постачальника зараховує (enlist) кошти на рахунок постачальника;

9 – банк постачальника повідомляє постачальника про зарахування коштів на його рахунок.

Ex 13.7. Read the text about ATMS and translate it using the list of words below.

To use the service of money transfers from a payment card holder's card account you need to:

1. Insert your card in the **ATM.**
2. Choose the language.
3. Make **visual check** for matching of the ATM and its elements with the image on the monitor.
4. **Confirm** to **continue the operation.**
5. Enter your **PIN-code** and push the **button INPUT** .
6. Choose a menu item – Cash transfer.
7. Enter 16 (sixteen) figures of the card number, to which you are going **to remit cash** from your card account.
8. Enter the sum, you would like to remit.
9. Confirm, that the card number and the **remitted sum** are **indicated** correctly.
10. On displaying on monitor screen that the transfer is **accomplished**, complete your work with the ATM.
11. **Remove** your card..

Ex 13.8. Match the words with their equivalents and then translate it.

a) ATM	1) ПІН-код
b) visual check	2) підтверджувати
c) to confirm	3) грошовий переказ
d) to continue the operation	4) візуальна перевірка
e) PIN-code	5) сума переказу
f) button INPUT	6) для продовження роботи
g) choose a menu item	7) забирати
h) cash transfer	8) банкомат
i) to remit cash	9) оберіть пункт меню
j) remitted sum	10) здійснювати
k) to indicate	11) здійснити грошовий переказ
l) to accomplish	12) вказувати
m) to remove	13) кнопка ВВЕСТИ

Ex 13.9. Read the text about payment cards in Ukrainian and then translate it into English, using the phrases given below.

Чому платіжні карти нашого банку?

Наш банк – один з найнадійніших і найдинамічніших банків України, що підтверджується провідними міжнародними **рейтинговими агентствами** Moody's Investors Service і Fitch Ratings.

Наш банк є принциповим членом **платіжних систем** Visa International і Mastercard Worldwide. Статус принципового члена є найвищим і свідчить про **повну відповідність** стандартам платіжної системи, а також про успішність і динамічність **розвитку карткового бізнесу банку**.

Банк має **розгалужену мережу філій і банкоматів**, що стрімко розвивається.

Клієнти банку можуть **безкоштовно проводити операції** більш ніж у 30 млн. торговельних і сервісних точках по усьому світу.

Клієнти банку можуть **знімати кошти** більш ніж у 30 тис. банкоматів по Україні і 850 тис. банкоматів по всьому світу, у валюті країни, у якій вони перебувають, не турбуючись про **декларування коштів** і **обмін валюти.**

Банк надає своїм клієнтам можливість відкриття рахунків у кожній із трьох валют (гривня, долар США, євро).

Клієнти банку одержують не тільки найвищу якість стандартних послуг, але й **широкий спектр** додаткових.

payment cards	платіжні карти
rating agency	рейтингове агентство
payment system	платіжна система
full compliance	повна відповідність
bank's cards business development.	розвиток карткового бізнесу банку
extensive branch and ATM network	розгалужена мережа філій і банкоматів
to execute operations	проводити операції
free of charge	безкоштовно
to withdraw cash funds	знімати кошти
to declare the currency	декларування коштів
to exchange the currency	обмін валюти
a wide range	широкий спектр

Ex 13.10. Read the phrases about Pension Card and translate them using the vocabulary below.

1. Our Pension card will allow you to…

- obtain professional financial advice and high quality services;
- save time and effort withdrawing your pension at any branch or from any ATM of Our Bank free of charge;
- gain extra income in the form of interest on the balance of your account;

- receive a text message on your mobile when your pension has been credited to your account;
- be assured that your funds are secure at Our Bank;
- get a bonus of 0,6 % on every purchase of goods or services with your payment card in Ukraine.

2. For your comfort you can choose from two pension programs:

The "Profitable" pricing package provides for extra interest on the account balance and free of charge cash withdrawals at Our Bank's cash desks and ATMs.

The "Free access" pricing package provides for free of charge cash withdrawals at all ATMs of Our Bank or any of our partner banks and interest on the account balance.

All you need to do is to apply to any of Our Bank's branches with your passport, pension certificate and individual taxpayer identification number - Our Bank will deal with all the Pension Fund related matters.

Ex 13.11. Match the words with their equivalents.

a) obtain professional financial advice	1) каса
b) high quality services	2) додатковий прибуток
c) branch	3) зняття готівки
d) extra income	4) якісне обслуговування
e) in the form of interest	5) залишок
f) balance	6) у вигляді відсотків
g) purchase of goods or services	7) покупка товарів чи послуг
h) cash desk	8) відділення
i) individual taxpayer identification number	9) отримувати професійну фінансову консультацію
j) pension certificate	10) пенсійне посвідчення
k) cash withdrawal	11) індивідуальний ідентифікаційний номер платника податків

Ex 13.12. Translate the following text using the below translated phrases.

Why the payment cards of the Our Bank?

The Our Bank is one of the most reliable and dynamically developing banks of Ukraine, which is confirmed by the leading international rating agencies Moody's Investors Service and Fitch Ratings.

The Our Bank is a principal member of Visa International and MasterCard Worldwide payment systems. Status of principal member is the highest one and testifies the full compliance with the payment system standards, as well as success and dynamism of the bank's cards business development.

The bank enjoys a dynamically developing extensive branch and ATM network.

Customers of the bank can execute operations free of charge in more than 30 million trade and service points worldwide.

Customers of the bank can withdraw cash funds in more than 30 thousand ATMs in Ukraine and 850 thousand ATMs all over the world in the national currency of the country of their stay with no obligation to declare or exchange the currency.

The bank provides its customers with an opportunity to open multicurrency accounts in any of three currencies (Hryvnias, US Dollars, Euro).

The bank's customers benefit not only from high quality of standard services, but from a wide range of additional services as well.

internet banking	інтернет-банкінг
financial portal	фінансовий портал
individual customer	індивідуальний клієнт
entrepreneur	суб'єкт підприємницької діяльності
remote management system	система дистанційного управління
personal account	власний рахунок
24-hr	цілодобово
SMS informing	SMS інформування
utility services	комунальні платежі
current account	поточний рахунок
card account	картковий рахунок
open joint-stock company	відкрите акціонерне товариство
"The State Export-Import Bank of Ukraine" (JSC Ukreximbank)	"Державний експортно-імпортний банк України" (ВАТ "Укрексімбанк")
tariff package	тарифний пакет
strong system of authentication and cryptography	системи суворої аутентифікації та криптографії

Keys

Ex 1.4

a–5	b–7	c–2	d–9	e–15	f–11	g–13	h–1	i–10	j–12
k–16	l–14	m–4	n–3	o–8	p–6				

Ex 2.4

a–3	b–2	c–9	d–4	e–1	f–8	g–13	h–11	i–15	j–6
k–7	l–14	m–9	n–12	o–10					

Ex 3.4

a-6	b-7	c-11	d-14	e-8	f-12	g-9	h-2	i-10	j-3
k-4	l-5	m-16	n-1	o-15	p-17	q-13			

Ex 4.4

a–7	b–13	c–8	d–6	e–11	f–16	g–19	h–17	i–2	j–20
k–18	l–4	m–9	n–3	o–1	p–12	q–15	r–5	s–10	t–14

Ex 5.4

a–7	b–6	c–9	d–11	e–8	f–3	g–4	h–2	i–1	j–5
k–12	l–13	m–10							

Ex 6.4

a–3	b–6	c–1	d–4	e–2	f–5	g–7	h–10	i–9	j–8

Ex 7.4

a–1	b–3	c–5	d–8	e–9	f–12	g–15	h–18	i–17	j–16
k–14	l–13	m–11	n–10	o–7	p–6	q–4	r–2	s–19	

Ex 8.4

a–23	b–11	c–6	d–2	e–14	f–3	g–13	h–9	i–17	j–21
k–8	l–18	m–1	n–22	o–10	p–4	q–15	r–12	s–19	t–7
u–16	v–20	w–5	x–24						

Ex 8.7

a–16	b–11	c–3	d–17	e–23	f–6	g–5	h–9	i–21	j–21
k–18	l–13	m–10	n–14	o–2	p–19	q–22	r–15	s–1	t–7
u–12	v–4	w–8							

Ex 9.4

a–6	b–7	c–8	d–9	e–3	f–1	g–5	h–4	i–2	j–10

Ex 10.4

a–7	b–1	c–2	d–8	e–4	f–9	g–6	h–5	i–10	j–3

Ex 11.4

a–11	b–3	c–13	d–2	e–4	f–1	g–6	h–8	i–9	j–7
k–5	l–12	m–10	n–14	o–15	p–16	q–17	r–18	s–19	

Ex 12.4

a–8	b–6	c–1	d–11	e–18	f–19	g–13	h–14	i–17	j–22
k–21	l–9	m–4	n–12	o–7	p–10	q–5	r–23	s–20	t–15
u–16	v–2	w–3							

Ex 13.2

a–11	b–12	c–7	d–8	e–1	f–3	g–4	h–5	i–2	j–9
k–1	l–10								

Ex 13.8

a–8	b–4	c–2	d–6	e–1	f–13	g–9	h–3	i–11	j–5
k–12	l–10	m–7							

Ex 13.11

a–9	b–4	c–8	d–2	e–6	f–5	g–7	h–1	i–11	j–10
k–3									

English-Ukrainian Vocabulary

A

a domestic and global financial network.	державна та світова фінансова мережа
abuse	зловживання
accessibility to customers	доступ для клієнтів
accumulating	збір
ad hoc application	спеціальна прикладна програма
adapt	пристосовуватися
adopt	приймати
advanced persistent threat	серйозна постійна загроза
adversary	противник
adverse business decision	несприятливе ділове рішення
affiliate with	приєднатися
agenda	програма (на день)
air gapping	заходи безпеки, що зазвичай приймаються для комп'ютерів, комп'ютерних систем або мереж, які мають бути дуже безпечними
alienate	відлякувати
allegiance	відданість
allow remote access to	дозволяти дистанційний доступ
ancillary	додатковий
anti-money laundering regulations	боротьба з відмиванням коштів
ascension	підйом
assets	активи
assistive technology	допоміжна технологія
assure	гарантувати
ATM card	картка для користування в банкоматах
audit trail	журнал контролю

B

back-end (back-office)	фоновий додаток
bank balance sheet	сальдо банківського рахунку
banking supervision	банківське спостереження
Banks and Savings & Loans	банківські та кредитні установи
basis risk	ризик, що загрожує діяльності банку
benchmarking	порівняльний аналіз
beneficiary	власник бенефіція
bidirectional	двунаправлений
borrower	позичальник

bring about standardization	запровадити стандартизацію

C

card account	картковий рахунок
cash flow	рух грошових коштів
clamour (for)	наполягати на
collateral	майнова застава
commercialize	перетворювати в джерело прибутку
compatibility	сумісність
compliance risk (nonconformance with	ризик недотримання правил
compromise	наражати на небезпеку
computer remittance	комп’ютерний грошовий переказ
computer rowdies	комп’ютерні хулігани
conduct business	вести бізнес
consolidate chore	концентрувати важку (рутинну) роботу
contactless market	безконтактний ринок
counterfeit	підробка
counterparty	контрагент (протилежна сторона)
coveted targets	бажані цілі
credibility	фінансова довіра
credit evaluator	кредитний експерт
credit risk	ризик, пов'язаний з несплатою кредиту
criminal acts in the banking system	злочини у банківській системі
criminal trespass	кримінальне посягання
cross-channel phishing	перехресний фішінг
currency exchange	обмін валют
current account	поточний рахунок
custodian	правонаступник
customer inquiries	запити клієнтів
customer loyalty	лояльність клієнтів
cyber crime	кібер-злочин
cyber crook	кібер-аферист
cyber-thief	кібер-злочинець
cyber-threat	кібер-загроза

D

data base	база даних
data mapping	відображення даних
declare the currency	декларування коштів
delicate technologies	удосконалені технології
demonetize	зменшувати ціну

deploy (against)	розгорнути (проти)
deposit checks	вносити чекові депозити
detect	викрити
digital banking	цифрові банківські операції
digital lifestyle	спосіб життя, що потребує цифрових технологій
diminished reputation	зруйнована репутація
disbursement	виплата
discretionary income	частина особистого доходу, що залишається після задоволення основних потреб
disintermediation	вилучення грошей з банківських рахунків
disruption	збій

E

embed	впроваджувати
emitter	джерело
encompass	охоплювати
end-user behaviour	поведінка кінцевих користувачів
entanglement strategy	стратегія утримання клієнтів
entrepreneur	суб’єкт підприємницької діяльності
entry-point	точка входу
erode	руйнувати
evaluate	оцінювати
examination	експертиза
exchange the currency	обмін валюти
exchange-rate fluctuations	коливання обмінних ставок
execute operations	проводити операції
existing procedures	поточні операції
expansion potential	потенціал розширення
expedite the time	пришвидшити час
extensive branch and ATM network	розгалужена мережа філій і банкоматів
extortion	вимагання

F

financial abuse	фінансове зловживання
financial data transactions	транзакції з фінансовими даними
financial portal	фінансовий портал
financial swindle	фінансове шахрайство
fixed-line infrastructure	інфраструктура провідних ліній
flexibility	гнучкість
focal points	основні напрямки (пункти)
foldable display	дисплей, що складається
foreign exchange	іноземна валюта

foreign exchange risk	валютний ризик
forge	фальсифікувати
franchise	франшиза
fraud	шахрайство
fraud detector	детектор шахрайства
fraudulent behaviour	шахрайські дії
free of charge	безкоштовно
from an economic perspective	з економічної точки зору
front-end (front-office) application	первинні (інтерфейсні) прикладні програми
frustrate	розчарувати
full compliance	повна відповідність
funds transfer	грошові перекази

G

governmental and private funds	державні та приватні фонди
granularities	ступінь деталізації
gross domestic product	валовий внутрішній продукт

H

hedging	хеджування
high-ranking bank executives	високопоставлене керівництво банку
hi-jack	зняття грошей з рахунку

I

identity theft	крадіжка чужої ідентичності
identity verification	перевірка особистих даних
illegally access	незаконно проникати
impact	впливати
impede	перешкоджати
inbound call	вхідний виклик
incur losses	зазнати збитків
individual customer	індивідуальний клієнт
infringement	порушення
interactions	взаємодії
interest rate	відсоткова ставка
interest rate risk	ризик внаслідок зміни відсоткової ставки
interest-related options	опції вибору відсотка
internet banking	інтернет-банкінг
iPhone check deposit	перевірка депозиту через айфон
issuer	емітент

K

keep customers in bill-payment relationships	утримати клієнтів завдяки їх потребам оплати рахунків

L

larceny	крадіжка
launch mobile check-deposit technology	запровадити технологію мобільної перевірки депозиту
legacy data	дані про спадщину
leverage of investment	залучення інвестицій
liabilities	зобов'язання
lines of business	сфера діяльності
liquidate	ліквідувати
liquidity	ліквідність
liquidity risk	ризик ліквідності
litigation	судовий процес
loans	позика
lurk	ховатися

M

m-commerce services	послуги мобільної комерції
mediation	посередництво
misappropriation	незаконне привласнення
mobile apps	мобільні програми
mobile banking	мобільний банкінг
mobile contactless payments	мобільні безконтактні платежі
mobile subscribers	абоненти мобільного зв’язку
morphing schedule	ланцюг банківських операцій, що змінюється
movement in interests rate	зміни у відсоткових ставках
mutual interest	взаємна зацікавленість

N

null and void	недійсний

O

obligor	боржник, дебітор
offense	правопорушення
offer financial transactions online	пропонувати фінансові операції в режимі онлайн
offer value added services	пропозиція сервісів із доданою вартістю
online banking households	родини – користувачі онлайн-банкінгу
online banks	онлайн-банки
online brokers	онлайн-брокери

open joint-stock company	відкрите акціонерне товариство
out-of-area credits	кредити іноземним особам
overdrafts	перевищення кредиту

P

paradigm	парадигма
payment cards	платіжні карти
payment cards	платіжні карти
payment system	платіжна система
penetrate	проникнути
perform stock trading	виконання торговельних операцій з акціями (цінними паперами)
perpetuate crime	вчиняти злочин
personal account	власний рахунок
perspective	перспектива
physical point of sale	фізичний пункт продажу (пристрій)
piggy-back	грабувати
prevention measures	заходи з попередження
proprietary algorithms	патентовані (власні) алгоритми

R

ramp up	зростати
rating agency	рейтингове агентство
receive online updates	отримувати онлайн-оновлення
reduce the needs	зменшити потреби
reducing fraud losses	зменшення втрат внаслідок шахрайств
remittance service	послуга переказу грошей
remote access	віддалений доступ
remote management system	система дистанційного управління
repricing risk	ціновий ризик
retention	утримання
revenue	прибуток
revenue stream	потік прибутку
roll out	з’явитися

S

sale-purchase transaction	транзакції купівлі-продажу
savvier	більш досвідчений
secured access to	гарантований доступ до
sensitive customer information	особиста інформація клієнта
service-oriented architectures (SOA)	схема для обслуговування широкого кола запитів
shareholder	акціонер

Single Euro Payments Area	Єдина Європейська Платіжна Зона
single industry	конкретна галузь промисловості
SMS informing	SMS-інформування
sophisticated internet banking capabilities	високотехнологічні можливості інтернет-банкінгу
sophisticated malware	шкідливе та складне для розпізнання програмне забезпечення (вірус)
sound decisions	правильне рішення
spectrum of maturities	діапазон строку платежу
stand-alone computers	автономні комп'ютери
«stop-list»	«чорний список»
strong system of authentication and cryptography	системи суворої аутентифікації та криптографії
supervision	нагляд, контроль
suppress	стримувати

T

take down	руйнувати
tangible and intangible	матеріальні / нематеріальні
tariff package	тарифний пакет
template	зразок
thumb impression	відбиток великого пальця
transfer bill	рахунок переказу
transmit images	передавати зображення

U

unauthorized access	несанкціонований доступ
unwind an account	закривати рахунок
upgrade effectiveness	покращити безпеку
user-friendly technology	легка у використанні технологія
utility bills	рахунки за комунальні послуги
utility services	комунальні платежі

V

verify the bona fides	перевірити чесні наміри
vest	наділяти
voiding of contracts	скасування контракту
vulnerabilities	слабкі місця

W

wide range	широкий спектр
wireless market	ринок безпровідного зв’язку
withdraw cash	знімати гроші

withdraw cash funds	знімати кошти

Y

yield curve risk	ризик у діапазоні кривої прибутковості

Ukrainian-English Vocabulary

SMS-інформування	SMS informing

А

абоненти мобільного зв’язку	mobile subscribers
автономні комп'ютери	stand-alone computers
активи	assets
акціонер	shareholder

Б

бажані цілі	coveted targets
база даних	data base
банківське спостереження	banking supervision
банківські та кредитні установи	Banks and Savings & Loans
безконтактний ринок	contactless market
безкоштовно	free of charge
більш досвідчений	savvier
боржник, дебітор	obligor
боротьба з відмиванням коштів	anti-money laundering regulations

В

валовий внутрішній продукт	gross domestic product
валютний ризик	foreign exchange risk
вести бізнес	conduct business
взаємна зацікавленість	mutual interest
взаємодії	interactions
виконання торговельних операцій з акціями (цінними паперами)	perform stock trading
викрити	detect
вилучення грошей з банківських рахунків	disintermediation
вимагання	extortion
виплата	disbursement
високопоставлене керівництво банку	high-ranking bank executives
високотехнологічні можливості інтернет-банкінгу	sophisticated internet banking capabilities
відбиток великого пальця	thumb impression
віддалений доступ	remote access
відданість	allegiance
відкрите акціонерне товариство	open joint-stock company
відлякувати	alienate
відображення даних	data mapping

відсоткова ставка	interest rate
власний рахунок	personal account
власник бенефіція	beneficiary
вносити чекові депозити	deposit checks
впливати	impact
впроваджувати	embed
вхідний виклик	inbound call
вчиняти злочин	perpetuate crime

Г

гарантований доступ до	secured access to
гарантувати	assure
гнучкість	flexibility
грабувати	piggy-back
грошові перекази	funds transfer

Д

дані про спадщину	legacy data
двунаправлений	bidirectional
декларування коштів	declare the currency
державна та світова фінансова мережа	a domestic and global financial network.
державні та приватні фонди	governmental and private funds
детектор шахрайства	fraud detector
джерело	emitter
дисплей, що складається	foldable display
діапазон строку платежу	spectrum of maturities
додатковий	ancillary
дозволяти дистанційний доступ	allow remote access to
допоміжна технологія	assistive technology
доступ для клієнтів	accessibility to customers

Е

експертиза	examination
емітент	issuer

Є

Єдина Європейська Платіжна Зона	Single Euro Payments Area

Ж

журнал контролю	audit trail

З

З економічної точки зору	from an economic perspective
З’явитися	roll out

зазнати збитків	incur losses
закривати рахунок	unwind an account
залучення інвестицій	leverage of investment
запити клієнтів	customer inquiries
запровадити стандартизацію	bring about standardization
запровадити технологію мобільної перевірки депозиту	launch mobile check-deposit technology
заходи безпеки, що зазвичай приймаються для комп'ютерів, комп'ютерних систем або мереж, які мають бути дуже безпечними	air gapping
заходи з попередження	prevention measures
збій	disruption
збір	accumulating
зловживання	abuse
злочини у банківській системі	criminal acts in the banking system
зменшення втрат внаслідок шахрайств	reducing fraud losses
зменшити потреби	reduce the needs
зменшувати ціну	demonetize
зміни у відсоткових ставках	movement in interests rate
знімати гроші	withdraw cash
знімати кошти	withdraw cash funds
зняття грошей з рахунку	hi-jack
зобов'язання	liabilities
зразок	template
зростати	ramp up
зруйнована репутація	diminished reputation

І

індивідуальний клієнт	individual customer
іноземна валюта	foreign exchange
інтернет-банкінг	internet banking
інфраструктура провідних ліній	fixed-line infrastructure

К

картка для користування в банкоматах	ATM card
картковий рахунок	card account
кібер-аферист	cyber crook
кібер-загроза	cyber-threat
кібер-злочин	cyber crime
кібер-злочинець	cyber-thief

коливання обмінних ставок	exchange-rate fluctuations
комп'ютерний грошовий переказ	computer remittance
комп'ютерні хулігани	computer rowdies
комунальні платежі	utility services
конкретна галузь промисловості	single industry
контрагент (протилежна сторона)	counterparty
концентрувати важку (рутинну) роботу	consolidate chore
крадіжка	larceny
крадіжка чужої ідентичності	identity theft
кредити іноземним особам	out-of-area credits
кредитний експерт	credit evaluator
кримінальне посягання	criminal trespass

Л

ланцюг банківських операцій, що змінюється	morphing schedule
легка у використанні технологія	user-friendly technology
ліквідність	liquidity
ліквідувати	liquidate
лояльність клієнтів	customer loyalty

М

майнова застава	collateral
матеріальні / нематеріальні	tangible and intangible
мобільний банкінг	mobile banking
мобільні безконтактні платежі	mobile contactless payments
мобільні програми	mobile apps

Н

нагляд, контроль	supervision
наділяти	vest
наполягати на	clamour (for)
наражати на небезпеку	compromise
недійсний	null and void
незаконне привласнення	misappropriation
незаконно проникати	illegally access
несанкціонований доступ	unauthorized access
несприятливе ділове рішення	adverse business decision
обмін валют	currency exchange
обмін валюти	exchange the currency

О

онлайн-банки	online banks

онлайн-брокери	online brokers
опції вибору відсотка	interest-related options
основні напрямки (пункти)	focal points
особиста інформація клієнта	sensitive customer information
отримувати онлайн-оновлення	receive online updates
охоплювати	encompass
оцінювати	evaluate

П

парадигма	paradigm
патентовані (власні) алгоритми	proprietary algorithms
первинні (інтерфейсні) прикладні програми	front-end (front-office) application
перевищення кредиту	overdrafts
перевірити чесні наміри	verify the bona fides
перевірка депозиту через айфон	iPhone check deposit
перевірка особистих даних	identity verification
передавати зображення	transmit images
перетворювати в джерело прибутку	commercialize
перехресний фішінг	cross-channel phishing
перешкоджати	impede
перспектива	perspective
підйом	ascension
підробка	counterfeit
платіжна система	payment system
платіжні карти	payment cards
платіжні карти	payment cards
поведінка кінцевих користувачів	end-user behaviour
повна відповідність	full compliance
позика	loans
позичальник	borrower
покращити безпеку	upgrade effectiveness
порівняльний аналіз	benchmarking
порушення	infringement
посередництво	mediation
послуга переказу грошей	remittance service
послуги мобільної комерції	m-commerce services
потенціал розширення	expansion potential
потік прибутку	revenue stream
поточний рахунок	current account
поточні операції	existing procedures
правильне рішення	sound decisions
правонаступник	custodian

правопорушення	offense
прибуток	revenue
приєднатися	affiliate with
приймати	adopt
пристосовуватися	adapt
пришвидшити час	expedite the time
проводити операції	execute operations
програма (на день)	agenda
проникнути	penetrate
пропозиція сервісів із доданою вартістю	offer value added services
пропонувати фінансові операції в режимі онлайн	offer financial transactions online
противник	adversary

Р

рахунки за комунальні послуги	utility bills
рахунок переказу	transfer bill
рейтингове агентство	rating agency
ризик внаслідок зміни відсоткової ставки	interest rate risk
ризик ліквідності	liquidity risk
ризик недотримання правил	compliance risk (nonconformance with
ризик у діапазоні кривої прибутковості	yield curve risk
ризик, пов'язаний з несплатою кредиту	credit risk
ризик, що загрожує діяльності банку	basis risk
ринок безпровідного зв’язку	wireless market
родини – користувачі онлайн-банкінгу	online banking households
розгалужена мережа філій і банкоматів	extensive branch and ATM network
розгорнути (проти)	deploy (against)
розчарувати	frustrate
руйнувати	erode
руйнувати	take down
рух грошових коштів	cash flow

С

сальдо банківського рахунку	bank balance sheet
серйозна постійна загроза	advanced persistent threat
система дистанційного управління	remote management system

системи суворої аутентифікації та криптографії	strong system of authentication and cryptography
скасування контракту	voiding of contracts
слабкі місця	vulnerabilities
спеціальна прикладна програма	ad hoc application
спосіб життя, що потребує цифрових технологій	digital lifestyle
стратегія утримання клієнтів	entanglement strategy
стримувати	suppress
ступінь деталізації	granularities
суб'єкт підприємницької діяльності	entrepreneur
судовий процес	litigation
сумісність	compatibility
сфера діяльності	lines of business
схема для обслуговування широкого кола запитів	service-oriented architectures (SOA)

Т

тарифний пакет	tariff package
точка входу	entry-point
транзакції з фінансовими даними	financial data transactions
транзакції купівлі-продажу	sale-purchase transaction
удосконалені технології	delicate technologies

У

утримання	retention
утримати клієнтів завдяки їх потребам оплати рахунків	keep customers in bill-payment relationships

Ф

фальсифікувати	forge
фізичний пункт продажу (пристрій)	physical point of sale
фінансова довіра	credibility
фінансове зловживання	financial abuse
фінансове шахрайство	financial swindle
фінансовий портал	financial portal
фоновий додаток	back-end (back-office)
франшиза	franchise

Х

хеджування	hedging
ховатися	lurk

Ц

цифрові банківські операції	digital banking
ціновий ризик	repricing risk

Ч

частина особистого доходу, що залишається після задоволення основних потреб	discretionary income
«чорний список»	«stop-list»

Ш

шахрайство	fraud
шахрайські дії	fraudulent behaviour
широкий спектр	wide range
шкідливе та складне для розпізнання програмне забезпечення (вірус)	sophisticated malware

Список літератури

1. Черноватий Л.М. Переклад англомовної технічної літератури. Електричне та електронне побутове устаткування. Офісне устаткування. Комунікаційне устаткування. Виробництво та обробка металлу / Л.М. Черноватий, В.І. Карабан, О.О. Омельянчук / За ред. Л.М. Черноватого і В.І. Карабана: навч. посіб. – Вінниця : Нова книга, 2006. – 296 с.

2. Корунець І.В. Теорія і практика перекладу / І.В. Корунець. – Вінниця : Нова книга, 2000.

3. Черноватий Л.М. Переклад англомовної економічної літератури / Л.М. Черноватий, В.І. Карабан, І.О. Пенькова – Вінниця : Нова книга, 2004.

4. Черноватий Л.М. Переклад англомовної економічної літератури. Економіка США: навч. посіб. / Л.М. Черноватий, В.І. Карабан, І.О. Пенькова, І.П. Ярощук. – Вінниця: Нова книга, 2007. – 416 с.

5. Коллін С.М.І. Англо-український словник комп'ютерних термінів. / С.М.І. Коллін; пер. з англ. В.В. Воробйова. – Х. : Кн-рекламне агентство «Ра», 2002. – 480 с.

6. Новий російсько-український політехнічний словник / Укл. М.П. Зубков. – Х. : Гриф, 2005. – 951 с.

7. Масловский Е.К. Англо-русский словарь по вычислительным системам и информационным технологиям. Ок. 55000 терминов / Е.К. Масловский. – М. : Руссо, 2003. – 824 с.

8. Жданова И.Ф. Новый англо-русский экономический словарь / И.Ф. Жданова. – 4-е изд., стереотип. – М. : Рус. яз. – Медиа: Дрофа, 2008 – VIII, 1025 с.

Навчальне видання

БАДАН Антоніна Анатоліївна

Переклад англомовних текстів
у галузі інформаційних банківських технологій

Навчальний посібник
для студентів спеціальності 6.020303 «Переклад»
денної та заочної форми навчання

Англійською та українською мовами

Роботу до видання рекомендувала проф. Т.О. Снігурова

Редактор Л.О. Пустовойтова

План 2013 р., поз. 1

Підп. до друку ___.___.___. Формат 60*84 1/16. Папір друк. №2
Друк – ризографія. Гарнітура Times New Roman. Ум. друк. арк. ____
Наклад 100 прим. Зам. № _____ Ціна договірна.

Видавничий центр НТУ «ХПІ»
Свідоцтво пор державну реєстрацію ДК № 3657 від 24.12.2009 р.
61002, Харків, вул. Фрунзе, 21.